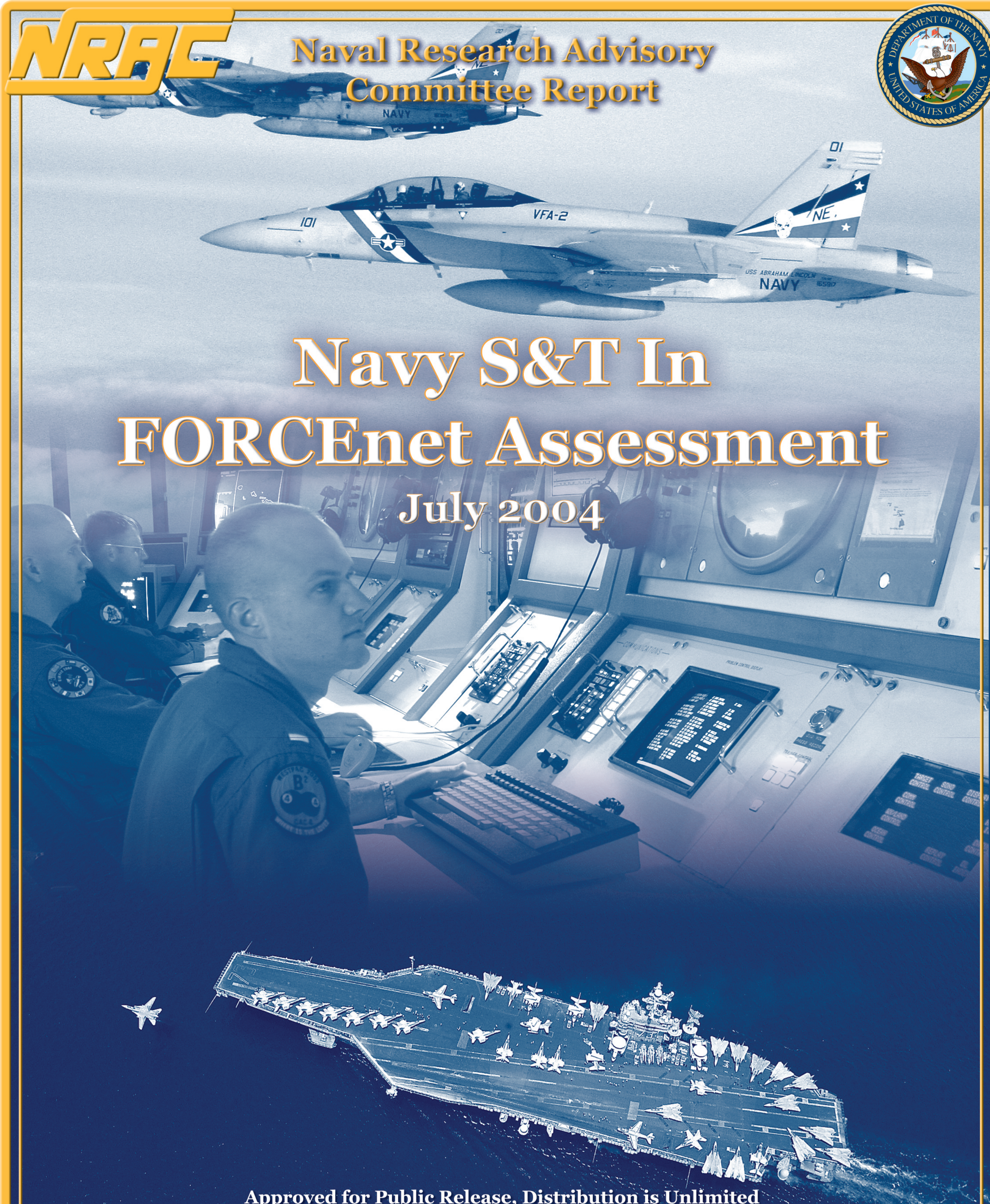
NRAC

Naval Research Advisory Committee Report

Navy S&T In FORCEnet Assessment

July 2004



Approved for Public Release, Distribution is Unlimited

OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)

NRAC 04-2

COPY NO.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **MAR 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Navy S&T In FORCENet Assessment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Research Advisory Committee 800 North Quincy Street Arlington, VA 22217-5660

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**74**	

This report is a product of the United States Naval Research Advisory Committee (NRAC) Panel on Navy S&T in FORCENet. Statements, opinions, recommendations, and/or conclusions contained in this report are those of the NRAC Panel and do not necessarily represent the official position of the United States Navy and United States Marine Corps, or the Department of Defense.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
04/02/04

2. REPORT TYPE
Group Study

3. DATES COVERED *(From - To)*
March 2003-March 2004

4. TITLE AND SUBTITLE
Navy S&T in FORCEnet

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
T. Betterton, C.J. Brinkman, P.A. Drew, P. Fratarangelo,
M.J. Gianelli, E. Horvitz, J.A. Johnson, J.B. Mooney,
N. Polmar, J.Y. Rodriquez, T.B. Smith, R.C. Spindel,
J.T. Tozzi, M. Unkauf, G.E. Webber,

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Research Advisory Committee
800 North Quincy Street
Arlington, VA 22217-5660

8. PERFORMING ORGANIZATION REPORT NUMBER
NRAC 04-02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Assistant Secretary of the Navy (Research, Development and Acquisition)
1000 Navy Pentagon
Washington, DC 20350-1000

10. SPONSOR/MONITOR'S ACRONYM(S)
ASN(RD&A)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Naval Power 21 articulates the current and future naval vision and operating concepts. This vision describes FORCEnet as the "integration of warriors, sensors, weapons, networks, and platforms." The CNO, in many public statements, has said that FORCEnet, as an element of Sea Power 21, will exploit emerging new technologies in communications, networking, and other areas, as well as fielded systems, to link the Sea Power 21 warfighting pillars of Sea Strike, Sea Shield, and Sea Basing.

The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN/RDA) requested that the Naval Research Advisory Committee (NRAC) conduct a study of the science and technology (S&T) requirements for FORCEnet.

Although the initial goal of the study was to explore the S&T underpinning for FORCEnet, the Panel found it necessary, because of the embryonic state of FORCEnet, to first evaluate the effectiveness of Navy efforts to define the FORCEnet vision and the implementation plans. In this report the Panel reviews the definition of FORCEnet, examines the progress achieved at this early stage, assesses current S&T development relevant to FORCEnet, makes recommendations for technology investment, and proposes a proactive approach to the structure and management of the FORCEnet effort.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dennis L. Ryan, III
UNCLAS	UNCLAS	UNCLAS	UU	67	**19b. TELEPHONE NUMBER** *(Include area code)* (703) 696-4875

This page intentionally left blank

Naval Research Advisory
Committee Report

Navy S&T In FORCEnet Assessment

July 2004

Approved for Public Release, Distribution is Unlimited

OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)

This page intentionally left blank

Table of Contents

This page intentionally left blank

Introduction

Naval Power 21 articulates the current and future naval vision and operating concepts. The Navy and Marine Corps have defined their respective Service strategies in Sea Power 21 and Marine Corps Strategy 21. This vision, which represents the foundation for the Chief of Naval Operations (CNO) Transformation Strategy, describes FORCEnet as the "integration of warriors, sensors, weapons, networks, and platforms." The CNO, in many public statements, has said that FORCEnet, as an element of Sea Power 21, will exploit emerging new technologies in communications, networking, and other areas, as well as fielded systems, to link the Sea Power 21 warfighting pillars of Sea Strike, Sea Shield, and Sea Basing. FORCEnet is expected to enable Navy and Marine Corps forces to operate as a highly integrated team in order to respond to the full spectrum of military operations.

The U.S. Marine Corps has implemented Expeditionary Maneuver Warfare (EMW), a capstone concept, that is the union of Marine Corps' core competencies coupled with their maneuver warfare philosophy, expeditionary heritage, sea basing, and the integration of operational and functional concepts.

FORCEnet will enable the increased effectiveness of Sea Strike, Sea Shield, Sea Basing, and EMW, as well as integrate naval operations. The Navy has devoted considerable effort to develop high-level FORCEnet concepts. Several Navy organizations have produced an extensive library of documents that explore FORCEnet ideas in terms of new capabilities being sought, and have looked at both ongoing and potential technology development programs for their relevance to FORCEnet.

The Assistant Secretary of the Navy (Research, Development, and Acquisition) (ASN(RDA)) requested the Naval Research Advisory Committee (NRAC) conduct a study of the science and technology (S&T) requirements for FORCEnet. The NRAC FORCEnet panel is made up of professionals in industry, academia, and retired Flag Officers, with many years of experience in Navy, Marine Corps and Coast Guard operations, program management, and technology development.

Although the initial goal of the study was to explore the S&T underpinning for FORCEnet, the panel found it necessary because of the embryonic state of FORCEnet to first evaluate the effectiveness of Navy efforts to define the FORCEnet vision and the implementation plans. In this report the panel reviews the definition of FORCEnet, examines the progress achieved in this early stage, assesses current S&T development relevant to FORCEnet, and makes recommendations for technology investment, and a proactive approach to the structure and management of the FORCEnet effort.

This page intentionally left blank

Executive Summary

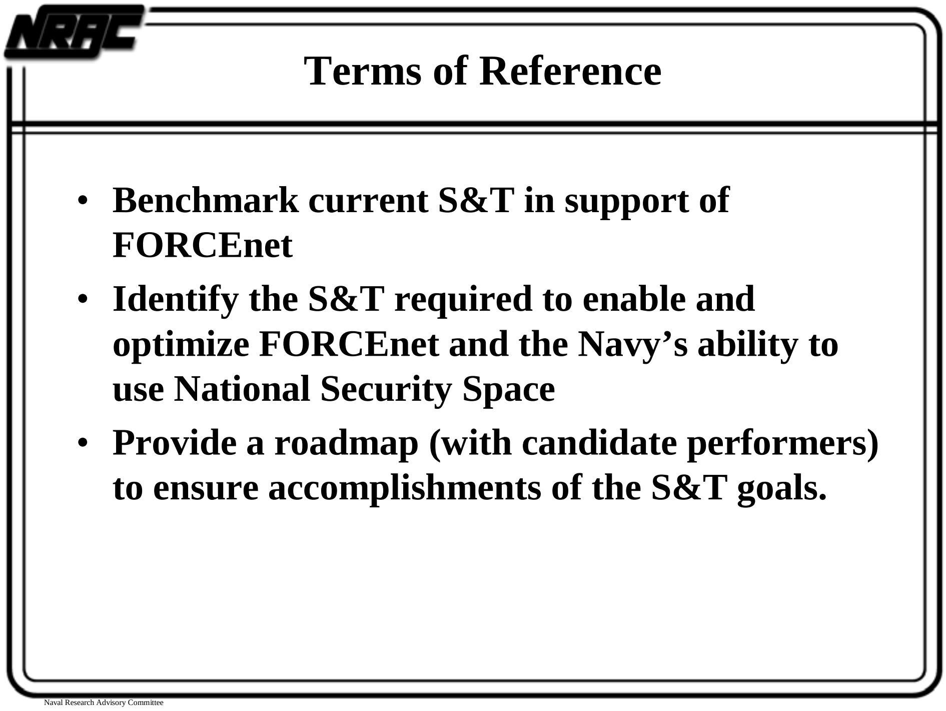
The NRAC FORCEnet Study Panel, which consisted of the members shown in Appendix A, reviewed the Architectural Vision document released 18 July 2003, and found that the report provides a strong overall vision. The Panel also reviewed the Campaign Plan released 3 June 2003 which identifies responsible naval organizations and the documents they are to prepare to provide the detail and implementation of the FORCEnet concepts. In April of 2004, a key document, containing FORCEnet implementation details will be released.

In evaluating the progress achieved, however, the Panel determined that the Campaign Plan documents released to date fail to translate Architecture visionary statements into a decisive fully funded plan for the implementation of FORCEnet accompanied by a strategic S&T roadmap. It also found that while many Navy activities and organizations are participating in the development of FORCEnet concepts, clear lines of accountability have not been established, and management roles for FORCEnet-related efforts remain ambiguous. An overarching System Engineering structure with authority to ensure properly phased integration of all FORCEnet related programs is needed. Most significant, the Navy thus far has not sought adequate funding for the S&T efforts that will be necessary, endangering prospects for success as well as credibility with the Office of the Secretary of Defense (OSD) and the other services.

The Navy and Marine Corps systems that provide FORCEnet capabilities must be compatible with the Department of Defense (DoD) Global Information Grid (GIG). The Panel thus urges the Navy to take a proactive role in the development of the GIG framework in order to ensure that the core networking standards and capabilities of the GIG satisfy the Navy FORCEnet implementation requirements.

In the area of the required technical infrastructure for FORCEnet, the Panel found that potentially critical details of FORCEnet architecture design and standards, as well as the processes needed for the transition of legacy systems, remain undefined. Current FORCEnet documents fail to address in enough detail the requirements for reliable and affordable connectivity among Navy and Marine Corps components. The FORCEnet effort also does not adequately address information assurance, security needs, intelligence, surveillance and reconnaissance (ISR), data fusion, and sensor management technology requirements. The Navy also has not provided sufficient investment in knowledge management and decision-aid technology needed to ensure real-time, echelon-appropriate decision support for FORCEnet. More generally, the Panel found insufficient investment in modeling and the analyses of scenarios and decision contexts. Information from such modeling and analysis efforts could serve to provide initial and ongoing guidance relative to the opportunities and challenges associated with alternate FORCEnet designs.

The Panel makes a number of specific recommendations to readdress these deficiencies. It also supports development of a FORCEnet Integration, Modeling and Simulation (M&S) Testbed, and new efforts to address requirements for network communications and security, knowledge management tools, and interfaces for legacy systems. In addition, the Panel found that beyond the current focus on large scale networking infrastructure and connectivity, FORCEnet S&T should probe architectures, protocols, and methods that support local, peer-to-peer networking, including mechanisms for discovery of components and services, ad hoc network configuration and maintenance, and robust sensor networks.



Terms of Reference

- **Benchmark current S&T in support of FORCEnet**
- **Identify the S&T required to enable and optimize FORCEnet and the Navy's ability to use National Security Space**
- **Provide a roadmap (with candidate performers) to ensure accomplishments of the S&T goals.**

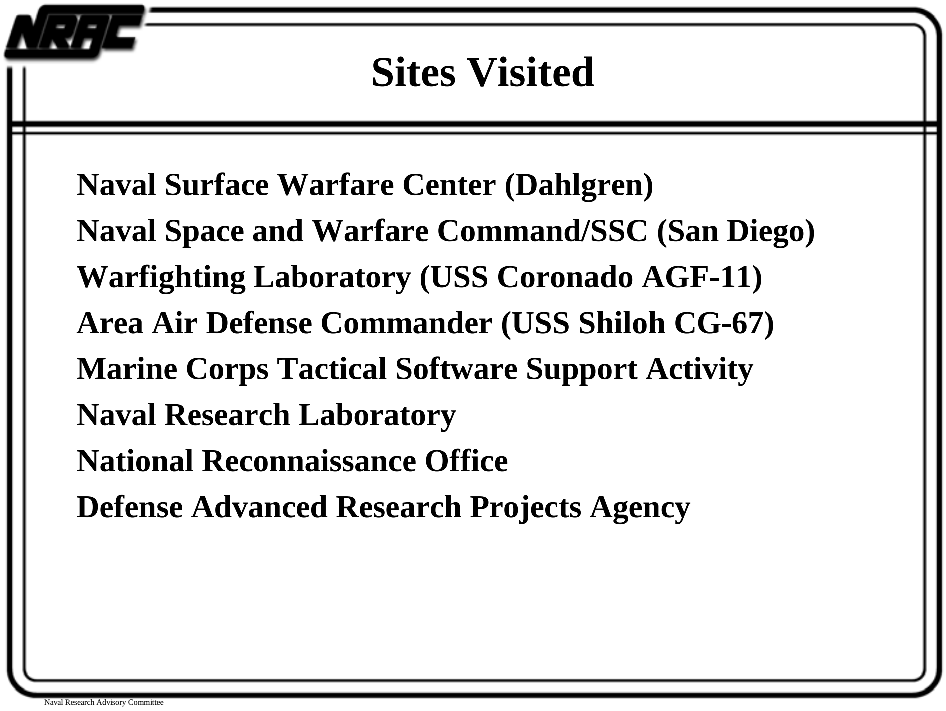
Naval Research Advisory Committee

Terms of Reference

In accordance with the ASN/RDA guidance, the Panel undertook to define the S&T initiatives required, and to propose additional options for leveraging the Navy's S&T efforts to meet Naval requirements for FORCEnet. The study's intent is to:

- Benchmark current S&T in support of FORCEnet;
- Identify S&T required to enable and optimize FORCEnet and the Navy and Marine Corps use of the National Security Space, and
- Provide a roadmap, citing candidate performers, to ensure that the S&T goals are met.

This page intentionally left blank



Sites Visited

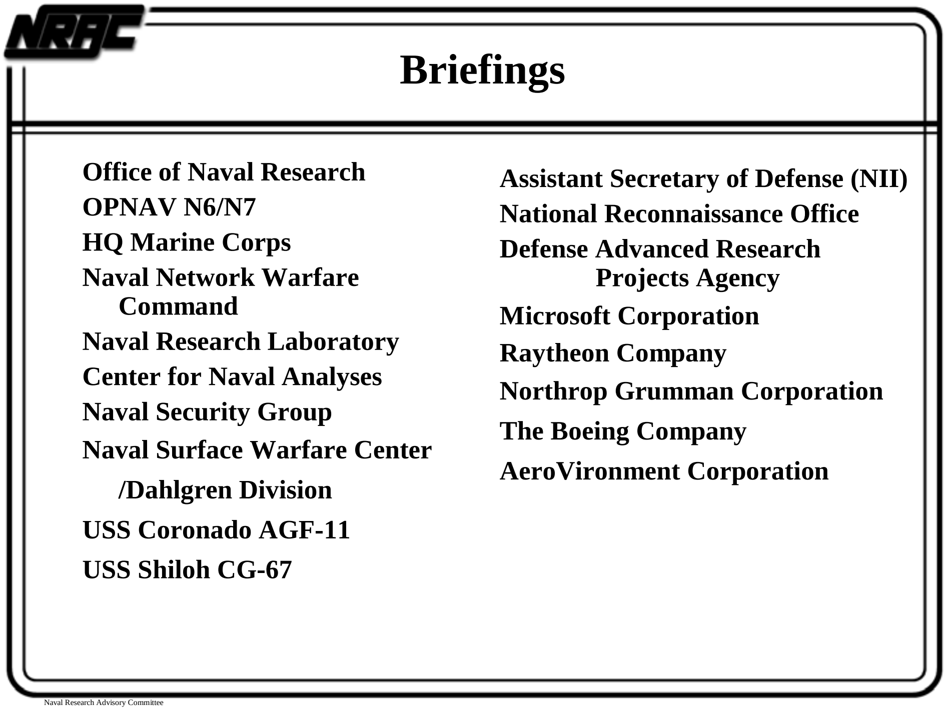
Naval Surface Warfare Center (Dahlgren)
Naval Space and Warfare Command/SSC (San Diego)
Warfighting Laboratory (USS Coronado AGF-11)
Area Air Defense Commander (USS Shiloh CG-67)
Marine Corps Tactical Software Support Activity
Naval Research Laboratory
National Reconnaissance Office
Defense Advanced Research Projects Agency

Naval Research Advisory Committee

Scope of Study

The Panel examined FORCEnet S&T issues through an extensive series of visits to Navy and Marine Corps fleet activities and laboratories, and received briefings by key officials from Navy and Marine Corps requirements, acquisition, and technology-development organizations, and DoD technology development agencies. The panel visited the Naval and DoD facilities that are sited above.

This page intentionally left blank



Briefings

Office of Naval Research
OPNAV N6/N7
HQ Marine Corps
Naval Network Warfare Command
Naval Research Laboratory
Center for Naval Analyses
Naval Security Group
Naval Surface Warfare Center /Dahlgren Division
USS Coronado AGF-11
USS Shiloh CG-67

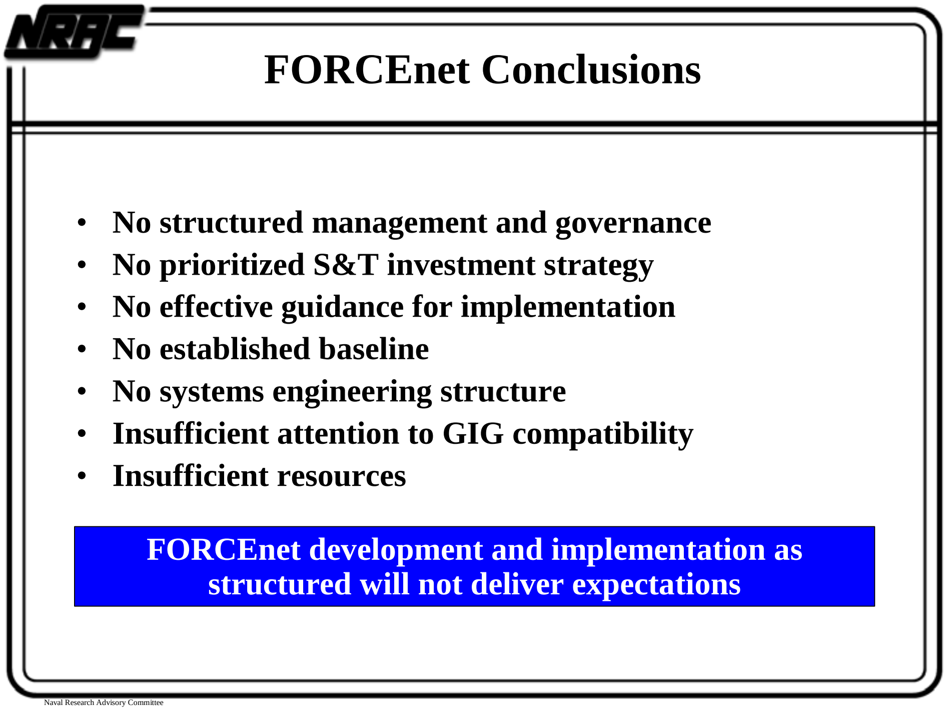
Assistant Secretary of Defense (NII)
National Reconnaissance Office
Defense Advanced Research Projects Agency
Microsoft Corporation
Raytheon Company
Northrop Grumman Corporation
The Boeing Company
AeroVironment Corporation

Naval Research Advisory Committee

The Panel received briefings on FORCEnet-related topics from government entities as well as prime contractors and systems integrators Northrop Grumman, Boeing, and Raytheon, as well as Microsoft, all of which are represented in the panel membership. The Panel also reviewed the Strategic Studies Group report on FORCEnet.

A complete listing of panel briefings is provided in Appendix B.

This page intentionally left blank



FORCEnet Conclusions

- **No structured management and governance**
- **No prioritized S&T investment strategy**
- **No effective guidance for implementation**
- **No established baseline**
- **No systems engineering structure**
- **Insufficient attention to GIG compatibility**
- **Insufficient resources**

FORCEnet development and implementation as structured will not deliver expectations

Naval Research Advisory Committee

Conclusions

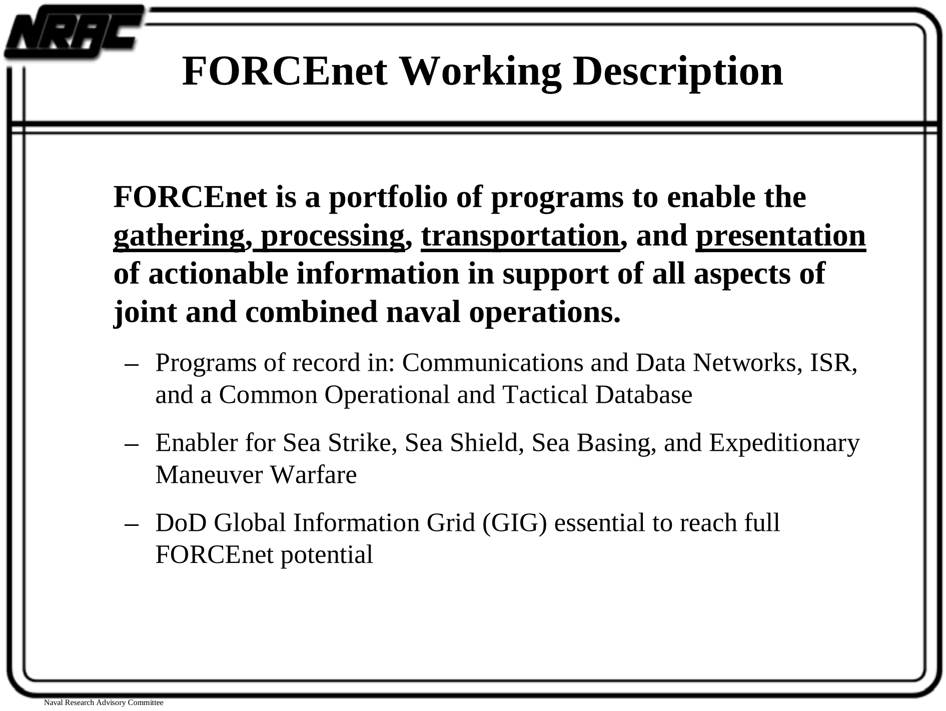
The Panel views S&T as a critical enabler for FORCEnet. However, in its evaluation of Navy progress on FORCEnet S&T, the Panel found no structured S&T strategy or roadmap. Despite the release of a FORCEnet Campaign Plan, it found that leadership roles for FORCEnet remain ambiguous. The lack of a coherent management structure evokes Adm. Hyman Rickover's observation, "When everyone is responsible, no one is responsible."

The Panel supports a clear and decisive leadership role for the Naval Network Warfare Command (NETWARCOM).

In the area of the technical infrastructure required for FORCEnet, the Panel determined that a FORCEnet architecture design, detailed standards, and the processes and procedures needed for the transition of legacy systems remain undefined. The Panel also noted that although the Space Warfare Systems Command (SPAWARSYSCOM) has been designated as the FORCEnet Chief Engineer, overarching system engineering authority and necessary resources have not been provided.

The FORCEnet effort does not adequately address information assurance and security needs nor ISR, data fusion, and sensor management technology requirements. Current FORCEnet documents fail to analyze and provide guidance on needs and means for establishing reliable and affordable high data-rate connectivity among Navy and Marine Corps components and joint forces. The Navy needs to increase its investment in decision-aid technology to ensure real-time, echelon-appropriate decision support, and in M&S in pursuit of a deeper understanding of the challenges and opportunities associated with developing and deploying new communications capabilities.

From an organizational perspective, the Panel found shortcomings in the Navy management structure and organization that will be required to address FORCEnet requirements. It noted in particular that DoD, Navy, and Marine Corps activities differ considerably in their perceptions of and expectations for FORCEnet. On the basis of numerous briefings on FORCEnet issues, that sea-service leaders and managers perceive FORCEnet as a panacea for shortfalls in technologies required to support Naval Power 21. The Panel members noted that the acquisition systems commands and Navy laboratories continue to aggressively pursue a number of Command, Control, Communications and Computer (C4) ISR programs, despite a lack of a coherent S&T strategy for FORCEnet. The Panel is concerned that deficiencies in current C4ISR capabilities cannot be identified without an established, shared, conceptual baseline for FORCEnet.



FORCEnet Working Description

FORCEnet is a portfolio of programs to enable the gathering, processing, transportation, and presentation of actionable information in support of all aspects of joint and combined naval operations.

– Programs of record in: Communications and Data Networks, ISR, and a Common Operational and Tactical Database

– Enabler for Sea Strike, Sea Shield, Sea Basing, and Expeditionary Maneuver Warfare

– DoD Global Information Grid (GIG) essential to reach full FORCEnet potential

Naval Research Advisory Committee

ForceNET

Working Description

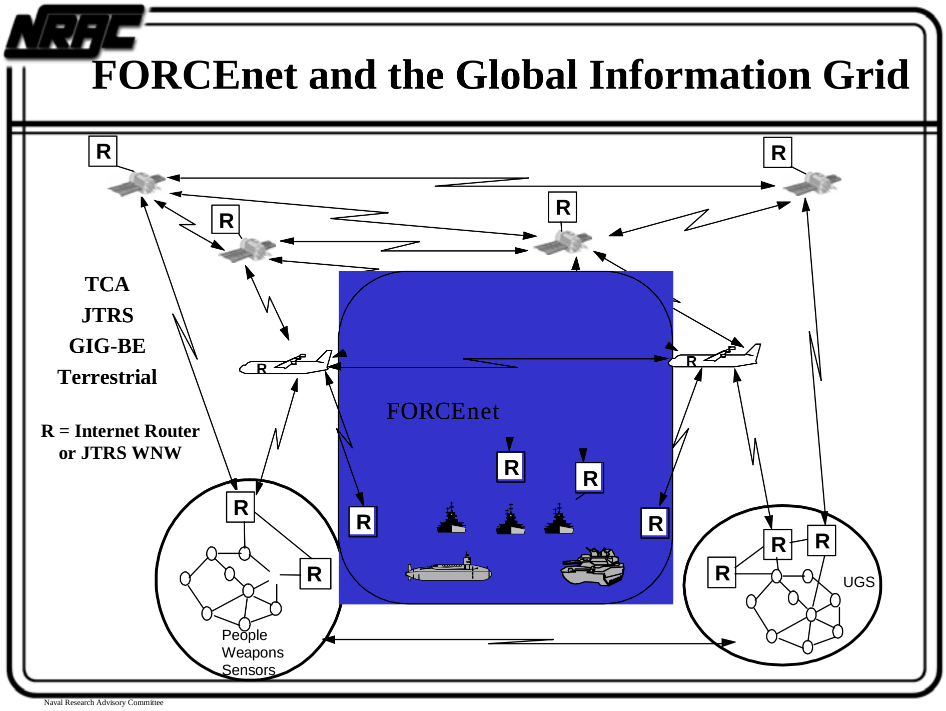
As noted above, the widely differing perceptions and expectations of FORCEnet presented an initial dilemma for the Panel in its efforts to assess S&T adequacy and a future investment strategy. The ambiguity and lack of precision in current Navy discussions and definitions of FORCEnet hampered the Panel's mission to recommend concrete S&T initiatives.

Panel members noted that Navy briefers, during one morning's session, described FORCEnet variously as a concept, a vision, an architecture, a group of programs, a battle-space environment, an organizing principle, a framework, an economic necessity, a Naval enabler of the GIG, and, a portfolio of initiatives, among others. The Panel found no common understanding or definition relating to FORCEnet implementation. Additionally, requirements for FORCEnet capabilities as generated by N6/7 continue to evolve—creating a moving baseline that did little to resolve the Panel's dilemma.

The Panel also noted that although FORCEnet reliance on and compatibility with the GIG is mentioned in the FORCEnet Campaign Plan, Navy briefers who addressed the Panel did not cite GIG compatibility as a major issue. In fact, numerous briefers did not understand the GIG framework and could not explain how FORCEnet would adapt to the GIG architecture and standards. The Panel considers utilization of the GIG to be necessary, but not sufficient in the formulation of FORCEnet. While Navy planning assumes that GIG functionality is in place, the impact of non-availability of the GIG in the five to seven year near term period, is not visible in Navy planning.

To address the aforementioned issues and provide the framework for an S&T investment strategy the Panel developed a "capabilities-based" description that captures both the scope of FORCEnet and the linkage to a wide range of programs of record. There are more than 150 programs of record that require review to establish their relevance. Additionally, although many Navy leaders compared FORCEnet to the Internet transport function, it became clear that the N6/7 capability documents, as well as the programs of record, represented a much broader scope.

For the purpose of the study, the Panel defined FORCEnet as a ***portfolio of programs to enable the <u>gathering</u>, <u>processing</u>, <u>transportation</u>, and <u>presentation</u> of actionable information in support of all aspects of joint and combined naval operations.*** FORCEnet encompasses programs of record in Communications and Data Networks (CDN), ISR, and a Common Operational and Tactical Database. It will also represent an enabler for Sea Strike, Sea Shield, Sea Basing, and EMW. Concurrent design and co-evolution of FORCEnet with the GIG standards and framework, and eventual exploitation of communication and programming interfaces with the GIG will be essential to permit FORCEnet to reach its potential.



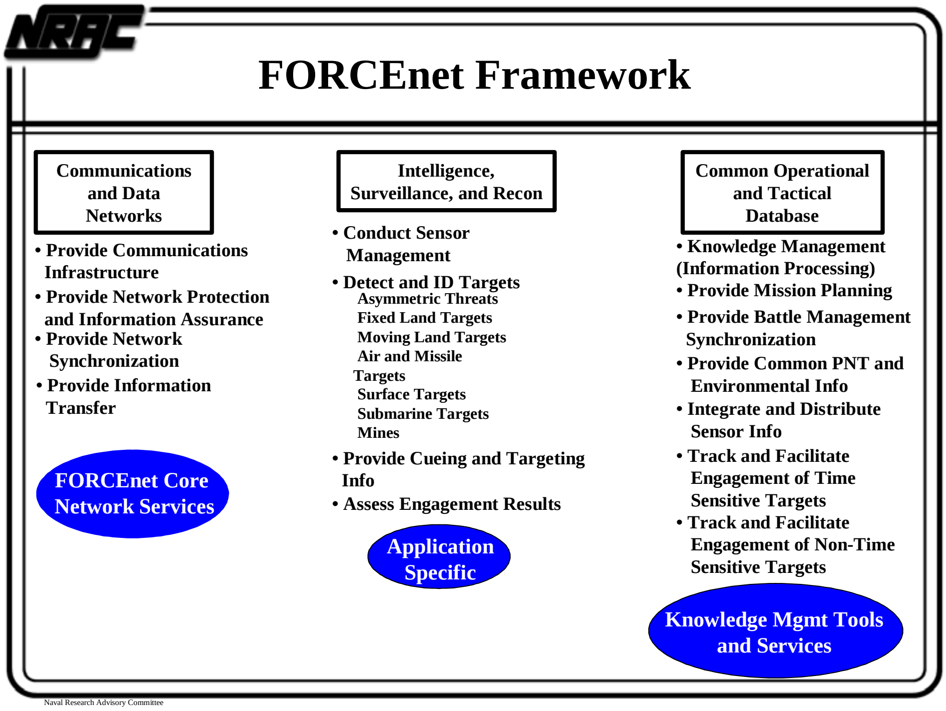
FORCEnet and the Global Information Grid

FORCEnet and the Global Information Grid

The Panel believes that the Navy must ensure that FORCEnet interface with the GIG to help to achieve interoperability and elaboration among the services. At the same time, the Panel recognizes that the GIG will not and cannot extend desired functionalities and bandwidth to dispersed Naval forces. FORCEnet must fill gaps left in GIG coverage as they occur for maritime operations and as illustrated in blue in Figure 11. For example, FORCEnet must provide support for Navy-unique battle groups, including submarines, and amphibious ready groups operating at sea.

The Navy and Marine Corps systems that provide FORCEnet capabilities must interface seamlessly with the DoD GIG. The Panel notes that the OSD is surveying all service C4ISR programs to determine if and to what degree they are compatible with the GIG. The Panel urges Navy officials to take a proactive role in the development of the GIG framework in order to ensure that the Navy's requirements are adequately addressed and that the GIG framework sets the core networking standards for FORCEnet.

This page intentionally left blank



FORCEnet Framework

Communications and Data Networks

- Provide Communications Infrastructure
- Provide Network Protection and Information Assurance
- Provide Network Synchronization
- Provide Information Transfer

FORCEnet Core Network Services

Intelligence, Surveillance, and Recon

- Conduct Sensor Management
- Detect and ID Targets
  - Asymmetric Threats
  - Fixed Land Targets
  - Moving Land Targets
  - Air and Missile Targets
  - Surface Targets
  - Submarine Targets
  - Mines
- Provide Cueing and Targeting Info
- Assess Engagement Results

Application Specific

Common Operational and Tactical Database

- Knowledge Management (Information Processing)
- Provide Mission Planning
- Provide Battle Management Synchronization
- Provide Common PNT and Environmental Info
- Integrate and Distribute Sensor Info
- Track and Facilitate Engagement of Time Sensitive Targets
- Track and Facilitate Engagement of Non-Time Sensitive Targets

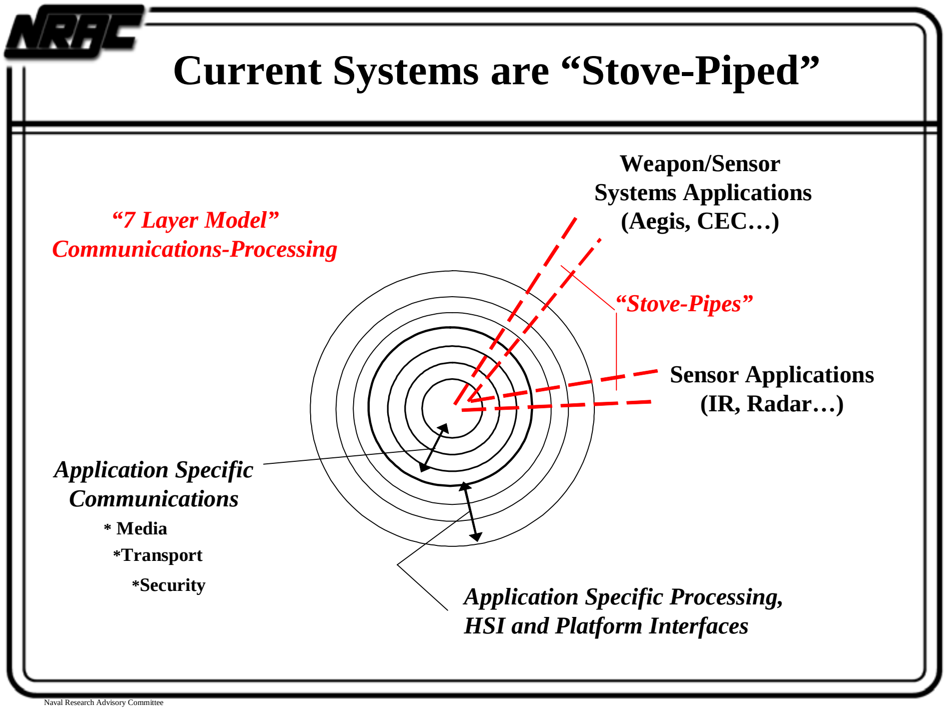
Knowledge Mgmt Tools and Services

Naval Research Advisory Committee

Capabilities and IT Framework

Using the aforementioned working description, the Panel reviewed the POM-06 Level 2 Hierarchy and made several modifications to further refine the FORCEnet framework from a capability perspective. The Panel then mapped the operational capabilities into an IT systems framework with attention to core network services, application specific functionality, and knowledge management tools and services as shown above.

This page intentionally left blank



Current Systems are “Stove-Piped”

“7 Layer Model”
Communications-Processing

Weapon/Sensor
Systems Applications
(Aegis, CEC…)

“Stove-Pipes”

Sensor Applications
(IR, Radar…)

Application Specific
Communications
* Media
*Transport
*Security

Application Specific Processing,
HSI and Platform Interfaces

Naval Research Advisory Committee

FORCEnet Common Networking Core

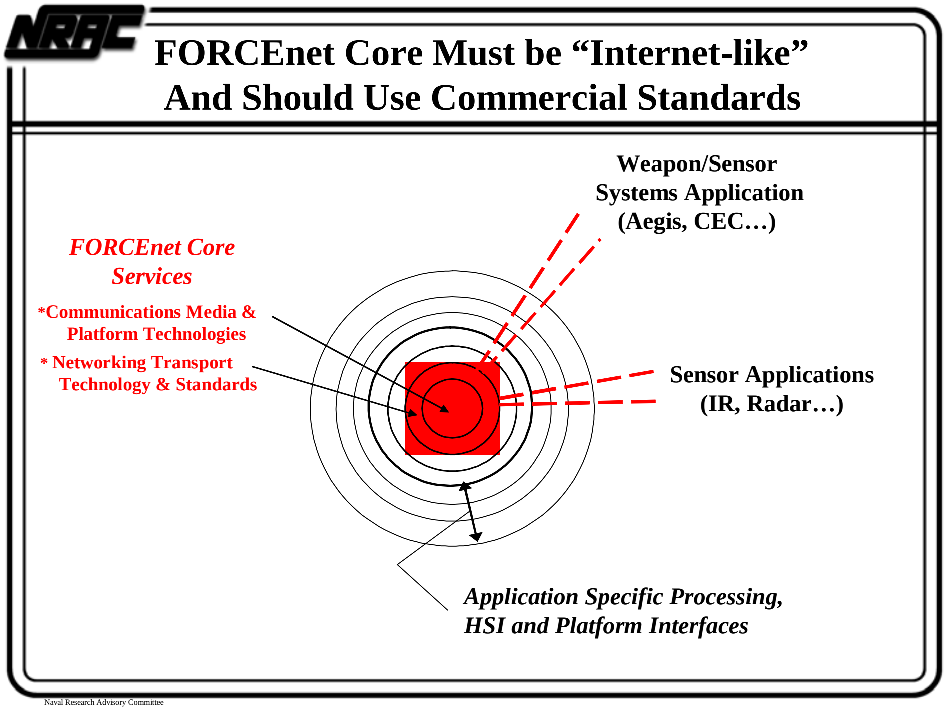
The Panel feels a common “networking core” is necessary to enable FORCEnet. The core must be both compatible with GIG standards and capable of meeting unique requirements for Navy operations.

Many existing Naval systems including weapons systems and C4ISR systems have been developed over time as stand-alone systems. As an example, each major system program usually developed its own dedicated sensor compliment, its own sensor data processing subsystem, its own dedicated communication subsystem, its own command and control system and perhaps its own dedicated weapon/response platform. This has often resulted in considerable duplication of capabilities particularly in the areas of information processing and communications.

Figures on pages 23-29 highlight, in a schematized manner, opportunities for achieving synergies and efficiencies via sharing of components and services, in contrast to traditional single-focused project designs. The figure above illustrates a sample decomposition of a networking and information-processing infrastructure into a seven-layer model. Each ring of the seven-layer model represents different elements of communications functions and information processing which are typically involved in a weapon system or C4ISR operation. The inner four rings of this layered model support communications-related processes. The outer three rings are associated with data and information processing, human and platform interfaces.

The inner most layers of the model involve the physical communications media which would include technologies such as radio frequency (RF), optical, acoustic, wires and cables, and even communications platforms technologies such as satellites and unmanned aerial vehicles (UAVs). The next layer in the model would include communications transport technologies such as Transmission Control Protocol/Internet Protocol (TCP/IP) (the current dominant protocol used for communication on today's Internet), followed by security related processes including such technologies as encryption and trusted computer processing technologies. The fourth ring in the model is associated with low level embedded signal processing and data access and distribution processing. Finally the outer three rings of the layered model represent various elements of higher level signal and information processing, as well as "human-system interface (HSI)" processing and display technologies, and processing associated with specific platform interfaces.

In the example illustrated, a hypothetical "stove-piped" weapon system would have its own dedicated "wedge" of specialized data processing and communications functions as shown by the red dashed wedges in figures on pages 23 and 25. These functions would be dedicated to only that weapon system and would span all communications and information processing from the weapons platform involved to the specific sensor subsystems that provided targeting and command control support.



NRAC

FORCEnet Core Must be "Internet-like" And Should Use Commercial Standards

Weapon/Sensor
Systems Application
(Aegis, CEC…)

FORCEnet Core Services

*Communications Media &
Platform Technologies

* Networking Transport
Technology & Standards

Sensor Applications
(IR, Radar…)

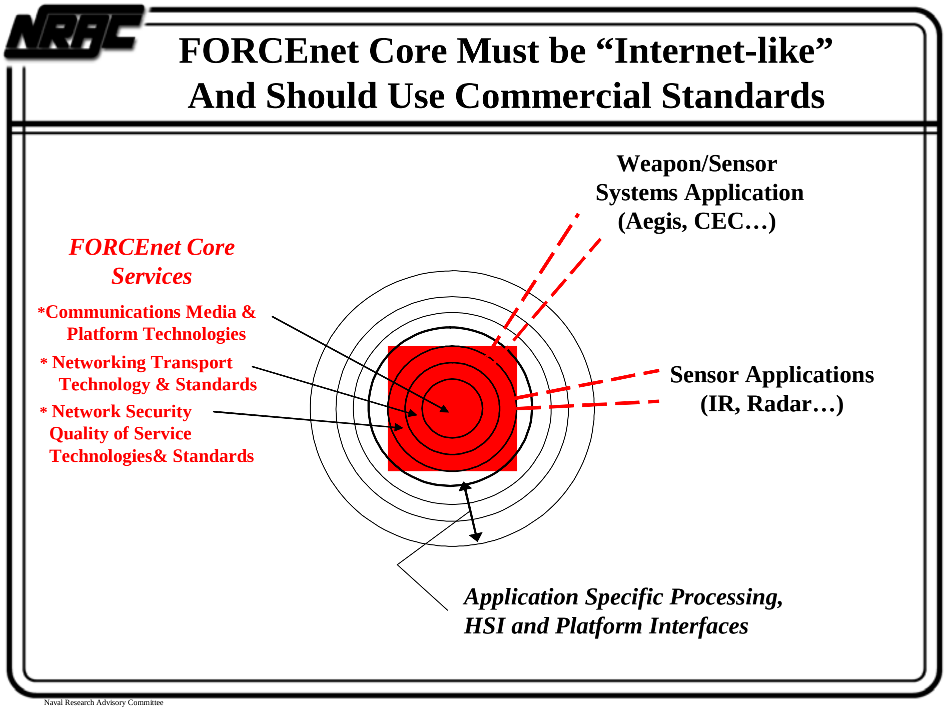
*Application Specific Processing,
HSI and Platform Interfaces*

Naval Research Advisory Committee

Considerable efficiencies in both cost and performance of weapons systems and C4ISR systems can be achieved if common standardized sets of communications and information processing functions can be addressed and used by multiple application systems. This would avoid duplication of capability and could also facilitate synergies between different systems, which could then access and take advantage of information derived by other systems using the common communications and processing infrastructure. It is clear that one of the primary strengths of the FORCEnet concept is to provide a common communications and processing infrastructure.

Again, using the seven-layer model representation of such an infrastructure, the figure above illustrates what the panel believes should be the central core of FORCEnet services. A common "core" of communications and networking services is necessary to enable FORCEnet as an operational concept. To this point, the FORCEnet operational model should reflect and build upon principles demonstrated and tested over time within the Internet.

This page intentionally left blank



FORCEnet Core Must be "Internet-like"
And Should Use Commercial Standards

FORCEnet Core Services

*Communications Media & Platform Technologies

* Networking Transport Technology & Standards

* Network Security Quality of Service Technologies& Standards

Weapon/Sensor Systems Application (Aegis, CEC…)

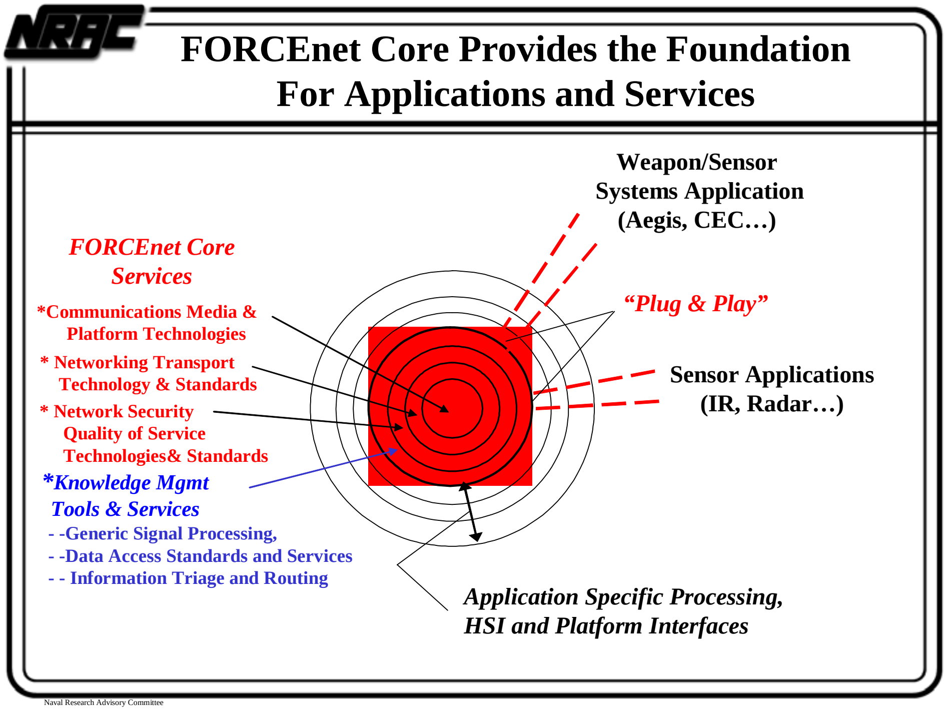
Sensor Applications (IR, Radar…)

Application Specific Processing, HSI and Platform Interfaces

Naval Research Advisory Committee

This figure illustrates that for the FORCEnet concept to be operationally viable, the inner core of standardized communications and networking services must be complimented by the next layer of services, which would include a standardized set of network security services as well as quality of service (QoS). Given the likely prospect of heterogeneous and time-varying changes in the bandwidth requirements of applications, and the inescapable competition by multiple applications for limited resources, QoS needs to be explored as a *multi-attribute* construct. This must include the ability to control such QoS dimensions as data rates, delivery guarantees, and the transmission of time-critical information before a specified deadline. It is worth noting that these types of standardized services have not typically been part of the Internet standards. For this reason, work needs to be done to evaluate and select standardized protocol strategies in these areas which can provide the necessary functions and services and which are in compliance with expected commercial products and uses in the future.

This page intentionally left blank



FORCEnet Core Provides the Foundation
For Applications and Services

Weapon/Sensor
Systems Application
(Aegis, CEC…)

FORCEnet Core
Services

*Communications Media &
Platform Technologies

* Networking Transport
Technology & Standards

* Network Security
Quality of Service
Technologies& Standards

**Knowledge Mgmt*
Tools & Services

- -Generic Signal Processing,
- -Data Access Standards and Services
- - Information Triage and Routing

"Plug & Play"

Sensor Applications
(IR, Radar…)

Application Specific Processing,
HSI and Platform Interfaces

Naval Research Advisory Committee

Knowledge Management Toolbox Services

The figure above illustrates that the final layer of the FORCEnet "common operating core" of services should incorporate standardized sets of "knowledge management" related tools and services which might be distributed around the FORCEnet network infrastructure but would be addressable as common services by application programs. These tools and services would be associated with such things as generic signal processing, standard distributed data access tools and protocols, "data mining" processes, and information "triage" and routing tools. In terms of knowledge management, the panel believes the Navy requires investment near-term in services and tools that will utilize the networking core and enable the development and interoperability of Naval C4ISR applications. Tools and services that are recommended to enhance tactical awareness, ISR, and knowledge development include the following:

- *Information triage & routing*: "Getting the right information to the right people at right time"; smart routing with best means and timing per identities, context, and content;

- *Fusion and decision support*: Synthesis, analysis, action-oriented presentation;

- *Global database servi*ces: Rich store with appropriate reliability and time stamps;

- *Expressive controls and representations*: Capture of the semantics of goals and situations for use in guiding automated triage, routing, fusion, and database operations.

As illustrated in the figure on page 29, once a common operating core is established, application programs including weapon systems, C4ISR applications, and various types of sensor subsystems could then effectively "plug into" the FORCEnet common operating core of network communications and information processing services using standardized application programming interfaces (APIs). Navy C4ISR and other application systems would utilize the networking core for common connectivity, security, and data-access services. Outside the common networking core, represented by the outer rings in the graphic, specific application systems would develop their own specialized functions for data processing, knowledge development, human-system interfaces, and platform interfaces as necessary. This approach would avoid expensive duplication of "stove-piped" systems and enable much greater synergies between systems for achieving enhanced operations capabilities.

While a conceptual decomposition of a communication and information processing infrastructure into such layers may be a useful abstraction, it is important to consider, at early phases of the design of a large scale transport system, interactions among layers in identifying desired capabilities of specific layers.

For example, requirements for expressive controls for QoS can only be identified with confidence by considering the use of actionable information in realistic decision contexts, in the setting of larger-scale resource usage considerations. To continue the example, after a specification of a design for QoS properties and controls has been completed, an analysis of the requirements at lower levels needs to be performed. That is, the design requirements, informed by needs at the application level, need to be potentially propagated into the fundamental protocols of lower layers. For the QoS example, it is likely that many ISR applications have varying time-criticality and bandwidth needs depending on the context. Such variation may make it valuable to design a low-level transport protocol that allows an application running at an outer layer of the infrastructure to make fast-paced quality of service requests, and that can, in turn, understand how to queue and triage the flow of data through the network.

As noted above, the types of standardized services we have called out have not typically been part of Internet standards. For this reason work needs to be done to evaluate and select standardized programming interfaces and protocols in these areas which can provide the necessary functions and services. The panel recommended that FORCEnet deliberation and design, in the realm of creating such programming interfaces and protocols, be done with awareness of academic and commercial efforts in the forms of recent efforts to develop Web ontologies and Web service protocols and interfaces. For example, the ongoing Semantic Web effort has sought to develop standard languages and predicates for communicating about content and services. The Microsoft .Net effort and related advanced technology efforts have led to the development of candidate protocols and interfaces for Web services. Such engineering efforts will likely be of value to the design of FORCEnet architecture, interfaces, and protocols.

Also, FORCEnet engineers need to consider the potential value of designing various protocols to directly harness, build upon, or simply be compatible with evolving commercial standards. If such a path is selected, the Navy, and DoD more generally, may wish to provide input to World Wide Web Consortium (W3C) standards bodies on interfaces and protocols rather than play the role of observer of deliberations about standards.

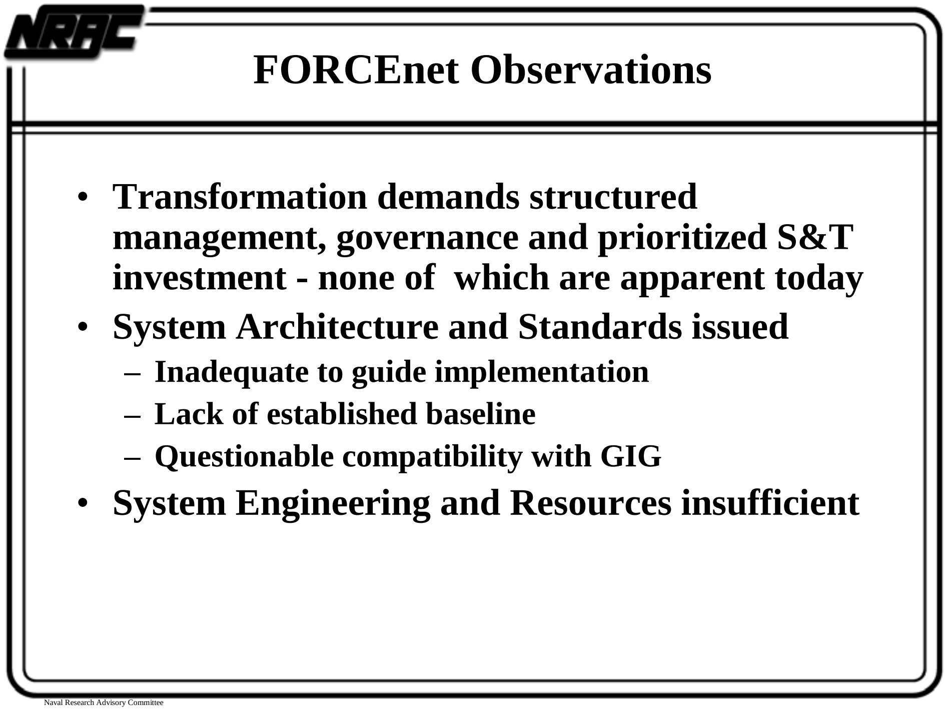
Analogous to opportunities for developing standards for the lower-level communication protocols, there are opportunities to develop standards for integrating components and services at higher levels of the infrastructure. Standards that allow components to declare their nature and abilities promise to facilitate the composition and robustness of applications and knowledge-management services. FORCEnet S&T efforts should include the review of efforts on such interfaces and standards in the academic and commercial realms. For example, within the Notification Platform research project at Microsoft Research, standard data models or schemas have been developed that allow such components as end-point devices and information sources to define themselves and to share out with other components on a network, information about information handling, processing capabilities. Thus, a standard device schema includes details, carried in an extensible Markup Language (XML) "blob", that includes information about the device's display properties, multimedia rendering abilities, audio alerting properties, bandwidth capabilities, receipt-response capabilities, and so on. Such definitional schemas give components (e.g., a new end-point device) the ability to share out with other components its properties, allowing the component to be efficiently annexed into a system without specialized hard coding.

Likewise, an XML schema for defining sensors, allows sensors to declare to a system or to the network more generally, key properties, including the nature of the information it can sense, its recent history of reliability in different contexts, the format and frequency of its transmissions, and so on. It is feasible, with the use of such rich definitional schemas and an overall supportive infrastructure that understands such schemas, to introduce sensors to a system or network overall, and have the systems or network understand what can be done with the sensors. At the time of usage or integration, a sensor can push information or be interrogated for information about its properties, via XML or other encoding.

FORCEnet S&T should include review of prior work and ongoing efforts on the creation of expressive definitional schemas on components. S&T should also explore Naval-centric innovations on interfaces, protocols, and schemas for defining and integrating such components and end-point devices, sensors, signal processing analyses, and decision support tools. FORCEnet engineers may wish to become aware and/or involved in the deliberations of W3C standards where appropriate.

Also, beyond considering FORCEnet as a large integrated network, FORCEnet designs and networking standards should provide methods that allow for the establishment of distant and local connectivity via peer-to-peer relationships, and via the formation of ad hoc networks. For example, FORCEnet designs should make it feasible for a fleet to establish and maintain a robust, efficient local peer-to-peer network that allows potentially rare high-bandwidth links to be shared with all participants. Peer-to-peer networks of distributed teams and components should likewise be easy to construct. It is important for FORCEnet engineers to be familiar with recent advances in the theory and practice of peer-to-peer networking in academic and commercial settings. In addition they should become knowledgeable with work on ad hoc networking, including, the investigation of ad hoc *sensor networks* to establish arrays of sensors that know how to report results of ongoing observations to sensor fusion components.

The deployment and refinement of new technologies, as advanced as they may be, can bring on new dependencies, vulnerabilities, fragilities, and unexpected behaviors via unmodeled interactions. The power and understandability of the Internet is based in part on the simplicity of the overall architecture and TCP/IP protocol. With new complexity comes the power to do more, but also the potential loss of clarity for prediction, troubleshooting, and security. For example, rich, expressive programming interfaces can support plug and play capabilities and provide great efficiencies for building and sharing components of applications and services. However, the same rich interfaces can present a myriad of entries for attack by adversaries or more neutral "hackers." FORCEnet designs need to balance the potential complexity and thus opacity of rich interfaces and services with the clarity and predictability associated with straightforward architectures and protocols.



FORCEnet Observations

- **Transformation demands structured management, governance and prioritized S&T investment - none of which are apparent today**
- **System Architecture and Standards issued**
  - **Inadequate to guide implementation**
  - **Lack of established baseline**
  - **Questionable compatibility with GIG**
- **System Engineering and Resources insufficient**

Naval Research Advisory Committee

Observations

While the Terms of Reference (TOR) approved for the NRAC FORCEnet study direct the Panel to focus on S&T, the Panel found it necessary to examine the overall FORCEnet structure. It found that achieving the full transformational benefit of FORCEnet required significantly greater attention in three areas: structured management, governance, and a process to prioritize S&T investment.

The FORCEnet Architecture & Standards documents issued to date accurately reflect the Navy's top-level FORCEnet strategy. However, those documents are inadequate to guide the detailed review, modification, and implementation of the more than 150 programs of record, representing billions of dollars of investment that should be associated with FORCEnet.

Expanded systems engineering will be required to provide effective synchronization and oversight of the programs of record essential to FORCEnet. A critical first step is the establishment of the reference baseline configuration. A gap analysis between a reference baseline and FORCEnet baseline 0 capabilities will establish goals and priorities. Validation of GIG compatibility also must be a key objective of the systems engineering effort.

FORCEnet, as a portfolio of programs centering on bringing new forms of coordination and actionable information to Navy operations, has the potential to truly transform Naval strategy and warfare. The scope of the Navy's investment in the programs of record associated with FORCEnet demands a management structure that clearly defines the roles and responsibilities of participating organizations and a plan for governance. Current S&T efforts, which are extensive, do not appear to represent a structured investment strategy. A process is required for prioritizing those efforts among all performing organizations.

Keystone documents, including the Campaign Plan, have been issued or are scheduled for completion by the second quarter of 2004. A further level of detail is required to translate the current underpinning to a formal FORCEnet implementation plan. The first step should be the establishment of a FORCEnet capabilities baseline from which to establish and measure time-phased incremental improvements.

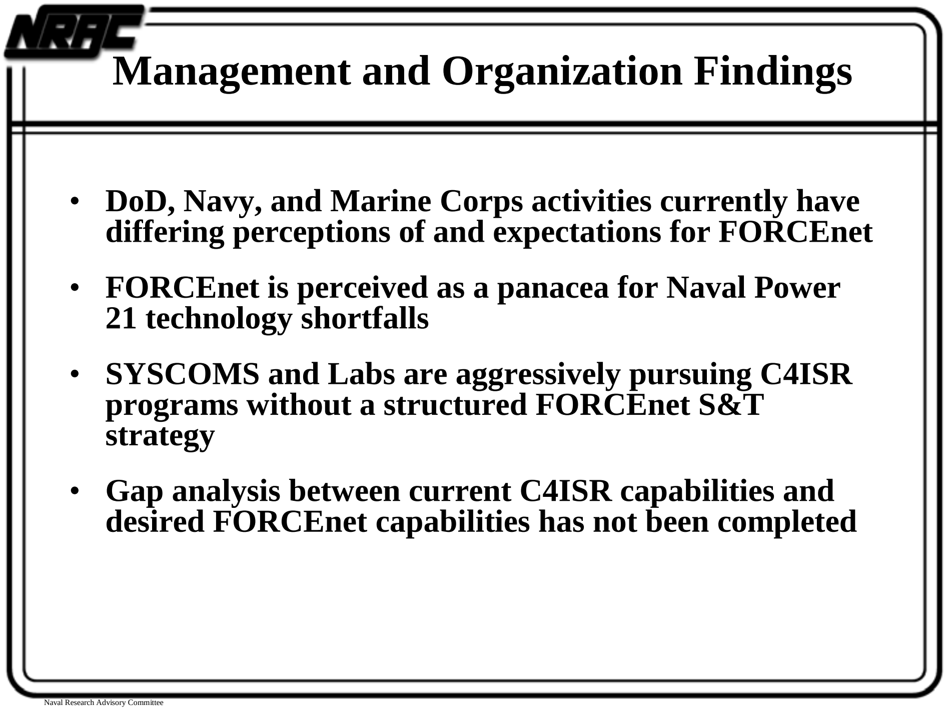
SPAWARSYSCOM has been assigned the responsibility as FORCEnet Chief Engineer, but the scope of that responsibility is not fully defined. The SPAWAR role appears to be limited to developing only the level of capability that is achievable with existing resources. FORCEnet implementation requires a significant and enduring systems engineering effort to properly manage, synchronize, and integrate the portfolio of programs essential to FORCEnet.

Findings

The findings of the panel from this study are grouped into three categories:

- Management and Organization
- ONR S&T Assessment
- Technical

This page intentionally left blank



Management and Organization Findings

- DoD, Navy, and Marine Corps activities currently have differing perceptions of and expectations for FORCEnet
- FORCEnet is perceived as a panacea for Naval Power 21 technology shortfalls
- SYSCOMS and Labs are aggressively pursuing C4ISR programs without a structured FORCEnet S&T strategy
- Gap analysis between current C4ISR capabilities and desired FORCEnet capabilities has not been completed

Naval Research Advisory Committee

Management and Organization

All Navy activities that briefed the Panel, including key FORCEnet participants, expressed differing views of FORCEnet, and the capabilities it should deliver. The Panel noted that many Navy officials assume that programs managed by their commands are elements of FORCEnet and, if funded, would be key components of Naval Power 21.

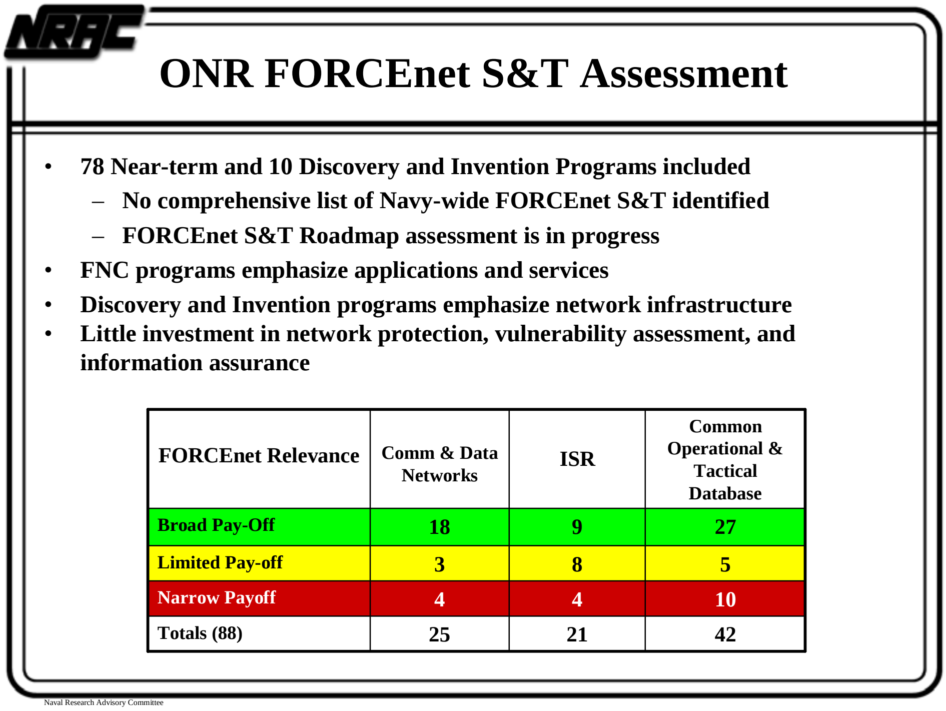
While the FORCEnet Campaign Plan eventually will be adopted Navy-wide, the Panel believes that the need for a shared vision will be resolved by the completion and dissemination of the supporting documents identified in the Campaign Plan. Because of the lack of a formal Navy definition of FORCEnet and list of programs identified as FORCEnet components, Navy and Marine Corps personnel and civilian staffs mistakenly believe that FORCEnet will address and correct perceived Naval Power 21 shortfalls.

The Panel finds a lack of synergy in the FORCEnet-related S&T work now underway within the Systems Commands (SYSCOMs) and laboratories. The SYSCOMs and laboratories are working aggressively to deliver improvements to current C4ISR programs without a structured FORCEnet S&T strategy. Panel members support the designation of SPAWAR as the lead SYSCOM for systems engineering efforts, primarily because of its focus on warfare-systems integration.

The Navy's SYSCOMs and laboratories currently are pursuing enhancements for fielded C4ISR capabilities and introducing new programs without the benefit of a FORCEnet roadmap. Such a roadmap is required to enable effective exploitation of S&T and avoid duplication. As previously stated in this report, a FORCEnet current reference baseline is needed in order to identify future C4ISR requirements, adequately track the evolution of requirements, and allocate S&T investment in a cost effective manner.

The FORCEnet Campaign Plan details a Capability Evolution Description (CED). NETWARCOM will oversee the delivery of FORCEnet capability to the Fleet in incremental blocks whose definitions are shaped fundamentally by Fleet requirements, the FORCEnet Integrated Architecture and Standards (IAS), and results of concept-based experimentation and prototyping through sea trials. FORCEnet Block 0 Capability Definition, the first increment of the CED, will be derived from available material solutions to address capability shortfalls identified by Commander Second Fleet, Commander Third Fleet and NETWARCOM. The Panel recommends that this effort be preceded by a reference baseline of current C4ISR capabilities. A gap analysis using this reference baseline will reveal the most productive directions for S&T support.

The Panel received and reviewed a draft copy of the FORCEnet Baseline Initial Capabilities Document (BCID) dated 22 May 2003. The Panel concluded that while the document provides additional support and insights regarding the FORCEnet vision and concepts, it does not provide the details to adequately define a current reference baseline.



ONR FORCEnet S&T Assessment

- 78 Near-term and 10 Discovery and Invention Programs included
  - No comprehensive list of Navy-wide FORCEnet S&T identified
  - FORCEnet S&T Roadmap assessment is in progress
- FNC programs emphasize applications and services
- Discovery and Invention programs emphasize network infrastructure
- Little investment in network protection, vulnerability assessment, and information assurance

FORCEnet Relevance	Comm & Data Networks	ISR	Common Operational & Tactical Database
Broad Pay-Off	18	9	27
Limited Pay-off	3	8	5
Narrow Payoff	4	4	10
Totals (88)	25	21	42

Naval Research Advisory Committee

ONR Science & Technology Assessment

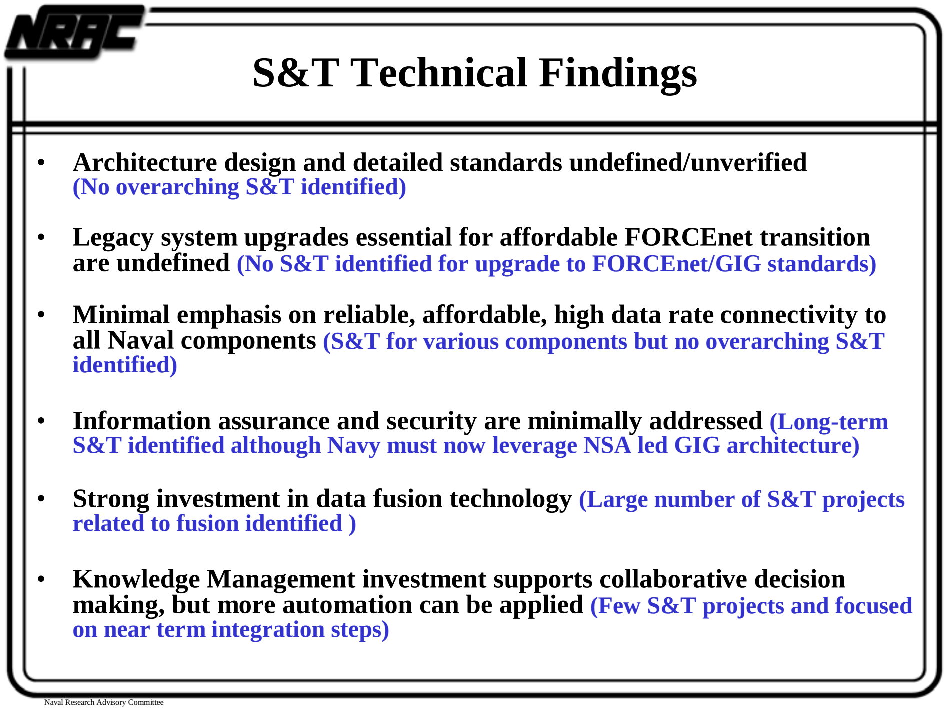
The Study Panel attempted to assess current Office of Naval Research (ONR) S&T initiatives in the context of the FORCEnet framework and the 21 functional capabilities. Since a comprehensive list of Navy-wide FORCEnet S&T was not identified, the Panel limited its evaluation to ONR initiatives only. The FORCEnet S&T Roadmap added 68 more Navy efforts to the Panel's list of ONR initiatives; however, analysis of technical focus was restricted to the ONR programs. The spreadsheet in Appendix C illustrates a breakout of the ONR S&T programs associated with the Common Operational and Tactical Database (COTD) Pillar. Each S&T project was given a qualitative assessment on a scale from 1 (little pay-off) to 3 (broad pay-off) by the panel as also illustrated in A1. Of the 88 initiatives evaluated, there were 78 current S&T programs and 10 long-term S&T thrusts. The evaluation summary of the 88 ONR S&T initiative is shown at the bottom of the above figure.

The technical findings from the Panel assessment concluded that:

- The S&T emphasis to date has been on services and applications, for example, ISR and COTD. This is likely due to the lack of definition in architecture and standards needed to define the needed infrastructure, the Knowledge Superiority Assurance (KSA) Future Naval Capability (FNC), and lack of a FORCEnet FNC.

- The long-term S&T thrusts emphasize FORCEnet infrastructure, supporting the view that the Navy S&T community recognizes the importance of developing the infrastructure, and that defining infrastructure and the supporting S&T poses a significant challenge.

- The Panel finds too little emphasis on information assurance and security associated with the evolution of FORCEnet. The transformational nature of FORCEnet carries the potential of both substantial warfighter benefits and vulnerabilities. The vulnerability assessment and the security/information assurance technology call for significant near-term S&T.



S&T Technical Findings

- **Architecture design and detailed standards undefined/unverified** **(No overarching S&T identified)**
- **Legacy system upgrades essential for affordable FORCEnet transition are undefined (No S&T identified for upgrade to FORCEnet/GIG standards)**
- **Minimal emphasis on reliable, affordable, high data rate connectivity to all Naval components (S&T for various components but no overarching S&T identified)**
- **Information assurance and security are minimally addressed (Long-term S&T identified although Navy must now leverage NSA led GIG architecture)**
- **Strong investment in data fusion technology (Large number of S&T projects related to fusion identified)**
- **Knowledge Management investment supports collaborative decision making, but more automation can be applied (Few S&T projects and focused on near term integration steps)**

Naval Research Advisory Committee

Technical Findings

In addition to attempting to evaluate the ONR S&T thrusts in depth, the Panel drew some broad conclusions on Navy S&T thrusts. These technical findings are summarized here.

- FORCEnet will build on communications and information standards to be developed by the GIG. Those standards are not sufficiently detailed, not verified by analysis/simulation, and likely incomplete.

- No S&T initiatives have been found that deal with adaptation of legacy systems to the emerging FORCEnet/GIG standards. Due to funding constraints, the early phases of FORCEnet will retain many legacy systems. Most legacy systems were designed as stand-alone non-interoperable “stove pipes,” and cannot provide the connectivity needed for network-centric operations. A study is needed to identify the legacy systems that will require upgrade to FORCEnet/GIG standards for network-centric operations. This is illustrated in Appendix C through a chart labeled “Selected Legacy Systems (SLS) integration required for FORCEnet transition.” S&T investment will be needed to upgrade the selected legacy systems, both to optimize their performance and to adapt the appropriate standards for networked operations and information sharing.

- The Navy has invested significant funds in S&T for various communications link enhancement technologies. Overarching S&T to provide reliable, high-rate connectivity to all platforms is not evident.

- Information Assurance (IA) and security architecture for FORCEnet must be compatible with that to be developed under the leadership of the National Security Agency for the GIG. Navy IA S&T must be directed to solving FORCEnet-peculiar issues.

- S&T investment in data fusion is significant, particularly efforts focused on real-time multi-source applications. However, more work to support the real-time dynamic integration of sensor nodes is required.

- Knowledge management technologies enjoy a reasonable level of investment, although current projects are focused mostly on first steps to integrated existing systems. The Panel believes that advances in such fields as data mining, advanced visualization, sensor fusion and decision support, and support for managing multiple tasks amidst interruptions need to be addressed.

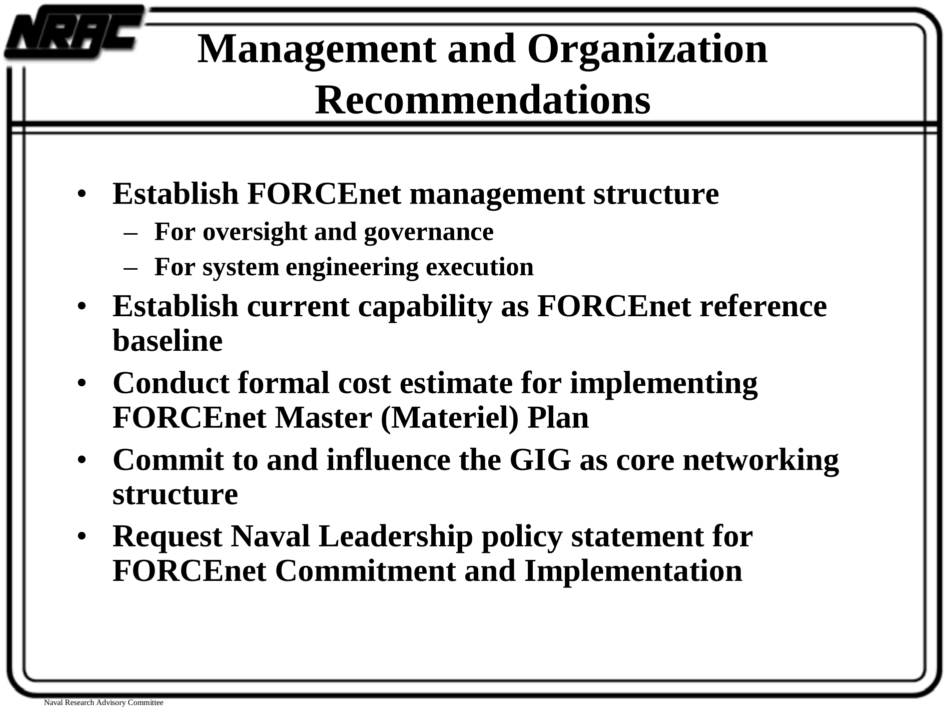
Recommendations

The Panel’s recommendations are grouped into three areas:

- Management and organization
- Technology investment
- S&T prioritization

Management and organization structures are required for the verification of standards, for comprehensive assessments and for the robust implementation of commitments. Second, technology investments must be programmed for systems integration and for the smooth transition to net-centric warfare. An S&T prioritization process is required for a FORCEnet roadmap.

This page intentionally left blank



Management and Organization Recommendations

- **Establish FORCEnet management structure**
  - **For oversight and governance**
  - **For system engineering execution**
- **Establish current capability as FORCEnet reference baseline**
- **Conduct formal cost estimate for implementing FORCEnet Master (Materiel) Plan**
- **Commit to and influence the GIG as core networking structure**
- **Request Naval Leadership policy statement for FORCEnet Commitment and Implementation**

Naval Research Advisory Committee

<u>Management and Organization</u>

Among its several recommendations to improve management of FORCEnet efforts, the Panel calls for establishment of a management structure that will be responsible for oversight and governance, and will ensure that required system engineering work is carried out. The Panel proposes specifically that the Navy designate the current fielded capability as the FORCEnet reference baseline. It recommends that the appropriate Navy organization develop a formal cost estimate for the implementation of the FORCEnet Master (Materiel) Plan. The Panel also urges the Navy to commit to and influence the GIG as the core networking structure, and recommends that the Secretary of the Navy (SECNAV)develop a FORCEnet Commitment and Implementation policy.

The successful development of FORCEnet will require several actions in the area of Management and Organization. These include resolution of issues raised in the Panel's Observations and Management and Organization Findings.

The Panel's specific management and organization recommendations include:

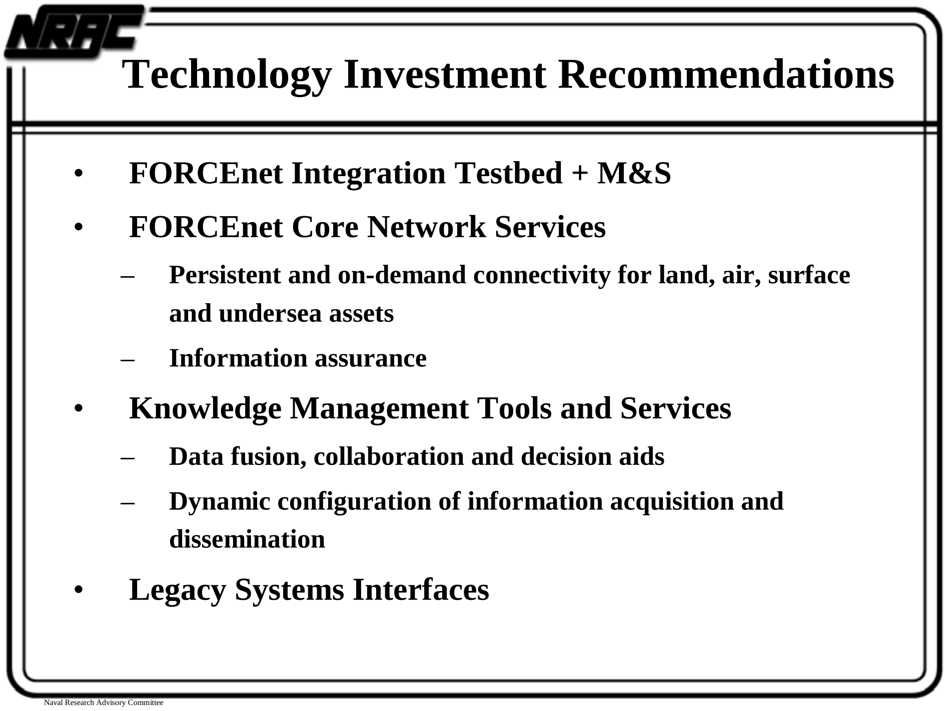
- Establishment of a governance structure for long-term FORCEnet oversight, implementation, and evolution. The structure should consist of a Flag/General officer steering committee and a working group at the O-4 to O-6 level. The structure, which would represent all Navy/Marine Corps stakeholders, would meet quarterly, and would coordinate with DoD activities (OSD, Naval Reconnaissance Office (NRO), Defense Advanced Research Projects Agency (DARPA), other services).

- Designation of the current C4ISR capabilities as FORCEnet reference baseline.

- Development of the formal FORCEnet cost estimate and deliberations leading to decisions regarding the size of S&T and acquisition investments. The decision process should list specific programs to be funded under the FORCEnet umbrella.

- Insuring that the FORCEnet configuration reflects GIG standards and that deployed Naval forces in key operating areas benefit directly from the GIG implementation. Exceptions necessary during the development stages of both systems, should be kept to a minimum.

- Drafting a SECNAV overarching policy statement on FORCEnet. Subsequently, the CNO and the Commandant of the Marine Corps (CMC) should issue a document implementing the formal instructions and directives needed to ensure execution of the FORCEnet Campaign Plan.



Technology Investment Recommendations

- **FORCEnet Integration Testbed + M&S**
- **FORCEnet Core Network Services**
  - **Persistent and on-demand connectivity for land, air, surface and undersea assets**
  - **Information assurance**
- **Knowledge Management Tools and Services**
  - **Data fusion, collaboration and decision aids**
  - **Dynamic configuration of information acquisition and dissemination**
- **Legacy Systems Interfaces**

Naval Research Advisory Committee

<u>Technology Investments</u>

The Panel recommends technology investment in four areas:

- Integration Testbed & M&S
- Core Network Services
- Knowledge Management Tools and Services
- Legacy Systems Interfaces

- **FORCEnet Integration Testbed and M&S**

The Panel urges the Navy to invest S&T funds in the development of a FORCEnet integration testbed for use in evaluating Naval requirements for FORCEnet networking core and application interface services. FORCEnet must establish a full-scale system integration test bed to define and verify FORCEnet requirements based upon the special operational needs of Naval C4ISR systems. Particular attention should be given to operational requirements of FORCEnet networking core and application interface services. These would include verifying DoN requirements and standards in the following areas:

- Network communications architecture and QoS requirements
- Security operational architecture including mandatory rule and role-based access control
- Common and reusable data access schemas and knowledge management tools and services
- Interface definition for legacy systems interoperability

As the deployment of new computing and networking capabilities involves the introduction of new dependencies and vulnerabilities, it will be critical to build models and simulations and to study test beds of key FORCEnet technologies. Beyond modeling and simulation, the panel recommends the use of red teams to continue to creatively probe vulnerabilities of solutions, so as to highlight potential weakness and fragilities.

The FORCEnet testbed can be rapidly established by building upon and enhancing the following capabilities:

- Naval Research Laboratory (NRL)’s ATDnet High Performance Networking Testbed (NRL Code 5590)
- SPAWAR’s applicable testbed capabilities applied to FORCEnet and linked to NRL’s GIG testbed
- NAVSEA’s Distributed Engineering Plant (DEP) Laboratory facilities.

A set of Department of the Navy (DON) C4ISR systems should be established as baseline for Block 1 FORCEnet capability and these should be integrated into the FORCEnet testbed for operational development and evaluation.

The FORCEnet integration testbed should provide real-time interfaces to the GIG test bed to ensure FORCEnet participation and compliance in developing GIG implementation standards. As the Navy determines its requirements for the FORCEnet networking core, it should also be a very pro-active participant in GIG development to ensure Navy/Marine Corps needs are met. The Panel also urges the Navy to invest in and utilize the NRL’s high performance networking test bed as a node in the GIG development test bed.

- **FORCEnet Core Network Services**

In addition to establishing an integration test bed evaluation of core network services (CNS) as described above, the Panel has identified two S&T areas for network services that will require additional investment to assure that DON operational capabilities. These include: persistent, ubiquitous, on-demand connectivity and information assurance.

Persistent, Ubiquitous Connectivity

Persistent, on-demand connectivity across air, land, surface and undersea assets requires increased S&T investment to meet Naval requirements. Deployed Naval forces typically are extended over broad open ocean and littoral regions, with surface elements beyond line-of-sight (BLOS) of each other. Current BLOS connectivity is carried out primarily via satellite communications (SATCOM), but constraints on shipboard antenna installations combined with satellite link-sizing limitations many times result in poor availability and lower than desired data rates.

The Navy has invested significant funds in S&T for various communications link enhancement technologies. However, overarching S&T to provide reliable, high-data rate connectivity to all platforms is not evident. The Panel recommends that an end-to-end connectivity strategy be defined and implemented to support FORCEnet objectives coupled with CONOPS that will define required data bandwidths.

An example of how to achieve this goal is using persistent airborne relays that can provide BLOS connectivity for battle-group elements and connectivity to the GIG. The need for a persistent airborne platform can be met by high-altitude, long- endurance UAVs such as Broad Area Maritime Surveillance (BAMS) and/or Global Hawk.

These platforms would be fitted with a communications relay package using the Joint Tactical Radio System (JTRS) Wideband Networking Waveform (WNW) for data rates up to 8 Mbps, a new "high-band version of WNW" for data rates to 100's of megabits per second (Mbps), and a SATCOM link to Transformational Satellite (TSAT) for GIG connectivity.

Because the airborne relay would operate much closer to the ship than a communications satellite, it could employ less-capable antennas, thereby simplifying integration and providing higher data rates and high reliability. A summary is illustrated in Appendix C under the title *Persistent, Ubiquitous Connectivity is FORCEnet Prerequisite*.

Information Assurance

The Panel strongly recommends that S&T investments in IA be significantly bolstered in terms of: near term development, capability assessments, requirements gathering, modeling and simulation test bed activity, integration with the NSA's IA plan, and compliance with the GIG. Current plans show IA as a long-term initiative only. However, current, net-centric warfare is critically dependent on this capability, and immediate Naval investment in this technology is woefully lacking.

The Panel recommends the Navy define the IA architecture and approach a priori as part of the core FORCEnet network services to ensure:

- Information confidentiality and integrity
- Utilization of a single "black" backbone network that can separate data at multiple security levels
- Information sharing with only authorized personnel and organizations, including ad-hoc coalitions
- Information availability at the time and place needed

The IA S&T investment should address the following required capabilities, also summarized in the chart titled – Communications and Data Networks: Information Assurance - in Appendix C.

> *Strong Authentication and Access Control* required to ensure only authorized people and systems have access to authorized information. Current systems are based on access control lists that are difficult to maintain in complex systems and don't capture policy or regulations directly. This capability must support dynamic coalition scenarios.

Policy and Role Based Access Controls using, for example, public key encryption technologies (PKI) and biometric technologies to ensure proper authentication and access.

Coalition Releasability. Dynamic relationships between Naval forces and Coalition forces require automated secure releasability of authorized information to Coalition partners using high assurance network boundary guard technologies. High assurance guard solutions of this type exist and should be evaluated against Naval requirements and enhanced and extended as necessary.

High Assurance Multi-Level Security Components. Certain parts of the computing systems supporting FORCEnet will have to be proven to be reliable and operational in a highly distributed and dispersed infrastructure. These will need to be implemented using high assurance components that provide protection from malicious attack and are capable of controlling information transactions at different security levels. High assurance computer technology of this type is currently commercially available but has been limited in its application because of the relatively small "niche" market that has used it to date. Naval S&T should focus upon the use and extension of this existing trusted computer technology for implementing these selected security critical functions that, for example, would include network guards, directories, certificate authority servers, cryptologic key management servers, and selected web and application servers.

Intrusion Detection is required to monitor and detect an unauthorized access. It should be deployed at the FORCEnet perimeter, network and at servers (hosts). S&T should also address the need to invest in approaches able to detect "slow and low" attacks that can span a long periods of time. These solutions (and attacks) will likely include the domain of "learning" technologies.

Availability and System Health. S&T investments are required to define proactive systems health monitoring capability that can detect anomalies in system behavior and predict failure or other undesirable behavior before a failure in the FORCEnet computing infrastructure system.

*Survivabilit*y. S&T investments should be made to define systems of systems level approach to ensuring that the network is resilient in the presence of failures, e.g. one component can fail, and the system is able to reconfigure itself without interruption of service. Current approaches are "patches" and frequently lead to ad-hoc redundancy and rely on weak situational awareness.

Insider Threats. This is a particularly hard problem since "insiders" have knowledge of security protocols and a valid account. Current approaches include running audits on "high value" targets under suspicion, but used sparingly due to large volumes of data generated by automated audits and lack of tools to process the resulting information. S&T into alternative approaches is warranted.

System of System Vulnerability Analysis. S&T investment is required to implement a strategy to determine whether or not FORCEnet information assurance and security protocols correctly implement the desired security policy. This requires various approaches to system testing, software engineering techniques and penetration analysis, including the use of formal method Knowledge Management Tools (KMT)and Services.

- **Knowledge Management Tools**

The category of KMT and Services covers all S&T investments required to transform the data and information available in FORCEnet into knowledge that aids the warfighter in decision making, in planning, and execution. The Panel recommends additional S&T investments to support improvements in data fusion and knowledge superiority.

Data Fusion

FORCEnet needs real-time integration and fusion of data from distributed, dynamically changing resources, with participants (sources, nodes and users) entering, leaving, and changing status or configuration. A data fusion chart can be found in Appendix C.

The current S&T plan includes significant investment in data fusion addressing many of the requirements of real-time, or near real-time, multi-source integration across multi-media sources (e.g. cross references of weather, imagery, sensor information). However, most of the programs are fairly narrowly defined focusing on a particular platform or application. There does not appear to be an overall architecture or strategy to provide an integration/fusion capability that can be reused across all types of information or sources. There is also significant investment in Combat ID of deceptive targets.

The Panel recommends that additional work be started to address some of the infrastructure needs of a dynamic, scalable, and robust data fusion capability. These programs would implement:

An overarching data fusion architecture and associated services that can be reused efficiently, and integrated dynamically in different application scenarios

Fusion Resource Management that can dynamically task and integrate groups of ISR assets to maximize information value in real-time.

Distributed Mobile Fusion management that provides the ability to configure a changing network, manage the distribution of data to the fusion service nodes, and distribute fusion across processing assets. Existing systems are mostly R&D prototypes and mostly for small numbers (1 to 5) of surveillance platforms and don’t operate in real-time. S&T to create a scalable, real-time capability is recommended.

Knowledge Superiority

There is a baseline of programs, associated with the Knowledge Superiority and Awareness Future Naval Capability, addressing some of the required technology. The Panel recommends this work be continued. Specifically, the current work is providing various decision aiding capabilities at the strategic, tactical planning and operational levels. These programs use various web technologies to integrate data through common data formats and visualization techniques. Collaborative decision making is provided primarily through updates of situational information and synchronization of views across multiple web-based operator terminals. There is also a strong level of current investment for advanced human system integration with advanced immersive, virtual reality environments, and some investment in advanced visualization to prevent information overload for operators. A knowledge superiority services summary can be found in Appendix C.

The panel recommends that ONR build on this base and increase S&T investments targeted toward increasing the amount of information that can be automatically processed and summarized. This must be done while accounting for uncertainty in the information, and to create more effective tools to help operators/analysts manage their workload in a dynamic planning and execution environment. Specifically, more S&T investments should be made in the following technology areas:

> *Agent-based information services* that monitor and search for information of particular relevance to an operator's task or stated profile; these services should also distribute information as appropriate throughout the system. This capability can be thought of as a proactive and more tailored version of a publish/subscribe service.
>
> *Data mining and knowledge discovery* algorithms can identify trends or patterns in volumes of structured or unstructured information. Much recent R&D has been done in this field, however, important issues for FORCEnet, such as knowledge discovery of time-sensitive data or anomaly detection still require additional S&T investment.
>
> *Decision aids* need to process real-time data feeds, providing results and recommendations based on partial or uncertain information. These systems must also be tailored to appropriate command and control structures, providing asynchronous decision making as well as synchronization and de-confliction.
>
> The current approach to task collaboration is being implemented primarily through chat rooms and ad hoc procedure management. *Automated workflow and task management* technology is required to support workgroups and coalitions netted across wide geographic distances; these systems should support person to person, person to system, and system to system work/task execution, and in compliance to FORCEnet decision making doctrine.

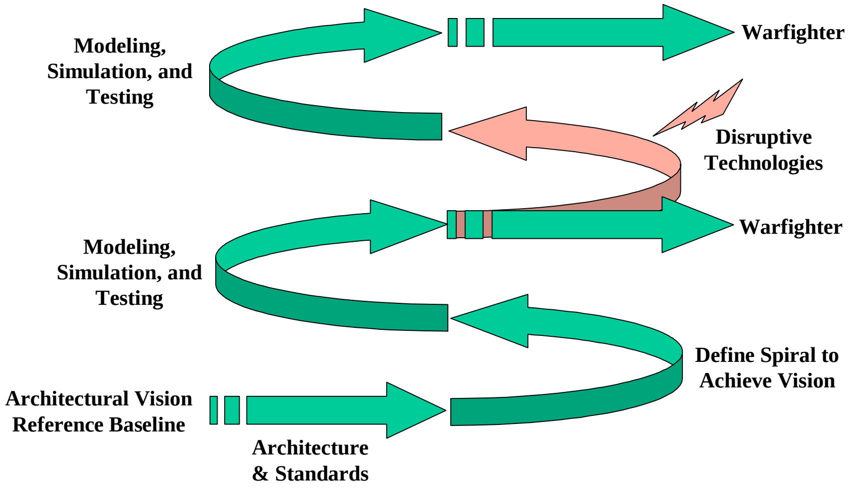
- **Legacy System Interfaces**

Due to funding constraints, the early phases of FORCEnet will retain many legacy systems. Most legacy systems were designed as stand-alone non-interoperable "stove pipes," and cannot provide the connectivity needed for network-centric operations. The panel feels that a study is needed to identify and inventory the legacy systems that will require upgrade to FORCEnet/GIG standards for network-centric operations.

Legacy System interface is also discussed in Appendix C *Selected Legacy System Integration Required for FORCEnet Transition.* S&T investment will be needed to upgrade the selected legacy systems, both to optimize their performance and to adapt the appropriate standards for networked operations and information sharing.

This page intentionally left blank

FORCEnet S&T Prioritization Process


Warfighter
Modeling, Simulation, and Testing
Disruptive Technologies
Warfighter
Modeling, Simulation, and Testing
Define Spiral to Achieve Vision
Architectural Vision Reference Baseline
Architecture & Standards

Naval Research Advisory Committee

FORCEnet S&T Prioritization Process

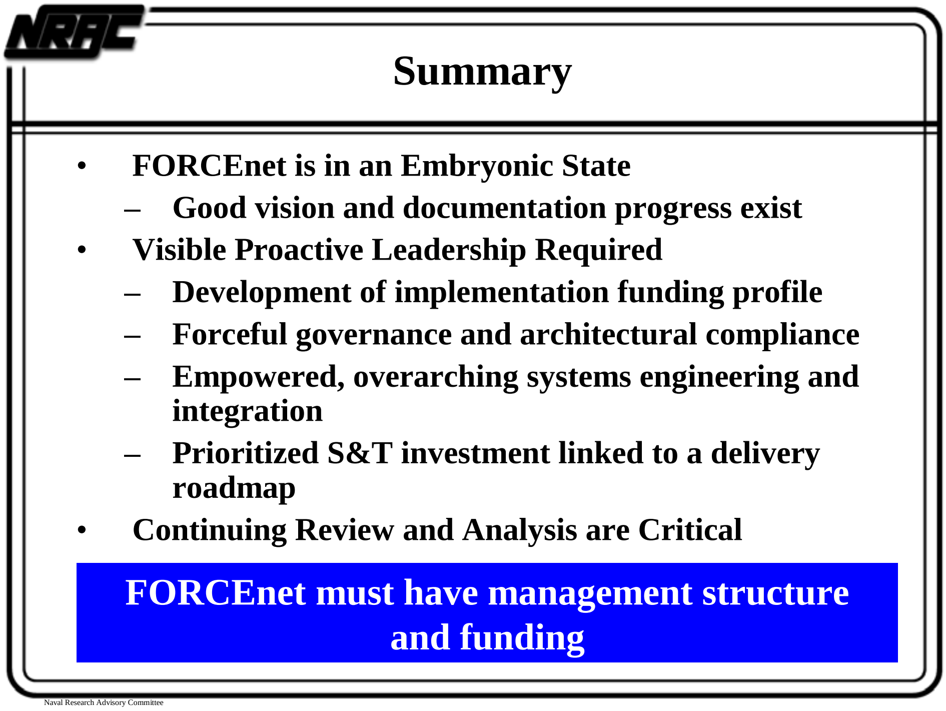
The figure above illustrates the Panel's process recommendation to develop FORCEnet and the S&T priorities. The S&T prioritization process starts with the definition of the architectural vision reflected in the FORCEnet Architectural Vision documents. The process then establishes the reference baseline through analysis, modeling, and simulation of current C4ISR systems and their capabilities.

The FORCEnet architecture, standards, and capabilities will be developed and evaluated through a spiral process for State-of-the-art and disruptive technologies. The same cycle of architecture-to-S&T-to-modeling-to-capabilities can be used to compare architecture and standard options, resulting in a best-value selection. The recommended integration, modeling, and simulation test bed is a key ingredient in this process

The S&T needed to implement the architecture, standards, and capabilities will be defined and a realistic spiral schedule determined. Modeling and simulation of the application of S&T products will determine the performance improvement relative to the reference baseline and the user. A "capabilities evolution" description will capture the resulting performance enhancements.

The cycle should be repeated periodically, or when the need arises, to achieve the FORCEnet vision.

This page intentionally left blank



Summary

- FORCEnet is in an Embryonic State
  - Good vision and documentation progress exist
- Visible Proactive Leadership Required
  - Development of implementation funding profile
  - Forceful governance and architectural compliance
  - Empowered, overarching systems engineering and integration
  - Prioritized S&T investment linked to a delivery roadmap
- Continuing Review and Analysis are Critical

FORCEnet must have management structure and funding

Naval Research Advisory Committee

Summary

In summary, the Panel's FORCEnet recommendations span three specific areas:

- Management and Organization
- Technology Investment
- S&T Prioritization

A well-defined management and organization for FORCEnet is essential to ensure that the architecture, standards and implementation plan are developed. Furthermore, a visible management and organization structure will empower the enterprise, drive activities, and establish accountability for results.

Technology investment must include system engineering and integration studies. The panel considers a FORCEnet test bed as an essential element for evaluating system engineering approaches and architectures.

In addition to system architectures, the panel views S&T prioritization as critical part of the FORCEnet roadmap. S&T prioritization must be coordinated with the spiral development and implementation of capabilities in the fleet.

The NRAC FORCEnet Panel finds that FORCEnet development is in a very early phase. Important decisions remain to be made about its course and consequences. Reviews and analyses must continue with persistence and responsible oversight.

Still, there is evidence of a clear vision for FORCEnet. Progress has been achieved in the development of documentation. The FORCEnet vision must be institutionalized with the development of a funding profile. Hiding behind the 150 plus programs of record totaling six plus billion dollars as a funding solution to implement FORCEnet is not realistic.

Visible, proactive leadership is required for FORCEnet if it is to succeed. The FORCEnet leadership must enforce compliance with the approved architecture and establish a reliable governance structure. The leadership must deploy integrated overarching systems engineering procedures and processes, and provide a well articulated science and technology roadmap that mandates prioritized science and technology investments. The viability and credibility of FORCEnet will be critically sensitive to the presence of persistent continuing review and analysis processes.

Appendix A
Panel Membership

Mr. Joseph Y. Rodriquez (Raytheon) – Chair

Ms. Teresa B. Smith (Northrop Grumman) - Vice Chair

RADM Tom Betterton, USN (Ret.)

Mr. Charles J. Brinkman (Northrop Grumman)

Dr. Pamela A. Drew (Boeing)

MajGen Paul Fratarangelo, USMC (Ret.)

Mr. Michael J. Gianelli (Boeing)

Dr. Eric Horvitz (Microsoft)

Dr. Joseph A. Johnson (Florida A&M)

RADM J.B. Mooney, USN (Ret.)

Mr. Norman Polmar (US Naval Institute)

Dr. Robert C. Spindel (APL/ University of Washington)

RADM John T. Tozzi, USCG (Ret.)

Dr. Manfred Unkauf (Raytheon)

Dr. George E. Webber (DigitalNet)

CDR James J. Shaw, USN, OPNAV N6111, Executive Secretary

This page intentionally left blank

Appendix B
Briefings

Office of Naval Research
ONR FORCEnet Process
JHU/APL FORCEnet/Human Factors
Force Transformation
Transformational Communications Architecture
ONR Naval Center for Space Technology
Future Combat Systems
Antenna Technologies
Precision Navigation and Timing and FORCEnet
ONR Commercial Technology Transition
Human Systems Integration

OPNAV
Sea Power 21
N6/N7 FORCEnet Perspective
TENCAP
Broad Area Maritime Surveillance BAMS UAV
Airborne Intelligence, Surveillance,
and Reconnaissance (AISR)
S&T Alignment with N6/N7
Naval Capabilities Process and Status

Defense Advanced Research Projects Agency
Command Post of the Future
DARPA Communications Initiatives
DARPA Littoral Naval Force Architecture
DARPA S&T
Network-Centric Operations and Joint Battle Command

National Reconnaissance Office
AS&T Organization Overview
Transformation Enabling Technologies
Hybrid Mirror X-SAT Effort
Joint Fires Network
CADP
AS&T Futures Laboratory Overview
Transformational Communications Architecture

NETWARCOM
Fleet FORCEnet Perspectives

Marine Corps
USMC FORCEnet Perspectives

ASD (NII)
ASN NII Investment Perspective

Center for Naval Analyses
CNA Communications Study

Naval Security Group
Future of Information Operations

Naval Research Laboratory
Virtual Reality Lab
Mother of All Databases Lab

Naval Surface Warfare Center, Dahlgren
Integrated Command Element (ICE)
Naval Fires Control System

Marine Corps Tactical Software Support Activity
Marine Corps FORCEnet: Way Ahead/Challenges

SPAWAR
SPAWAR FORCEnet Process
FORCEnet Overview
S&T Investments
FORCEnet Architecture & Standards
Command Center of the Future
PMWs 189, 157C2, 153, 156, 165, 173, 176, 179

USS Coronado (Sea-based battle laboratory)
Joint Fires Network
C41SR

USS Shiloh (Air Command Center)
Area Air Defense Commander

Raytheon
Raytheon Lasercom
Corporate S&T Initiatives
Cooperative Engagement Capability

Northrop Grumman
Overview
Command, Control, Communications
Networks for FORCEnet
Implications for Systems Design and Integration

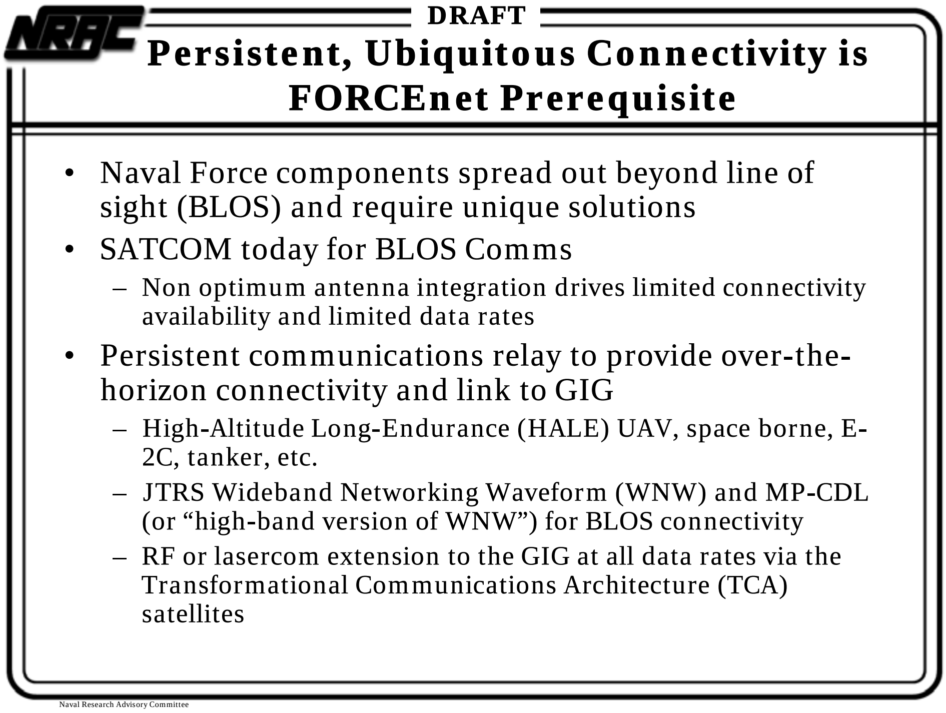
Boeing
FCS Common Architecture
Quality of Service in Ad Hoc Mobile Networks
Information Assurance
Data Fusion

AeroVironment, Inc.
High-Altitude Long Endurance for Naval Communications

This page intentionally left blank

Appendix C

Additional illustrations

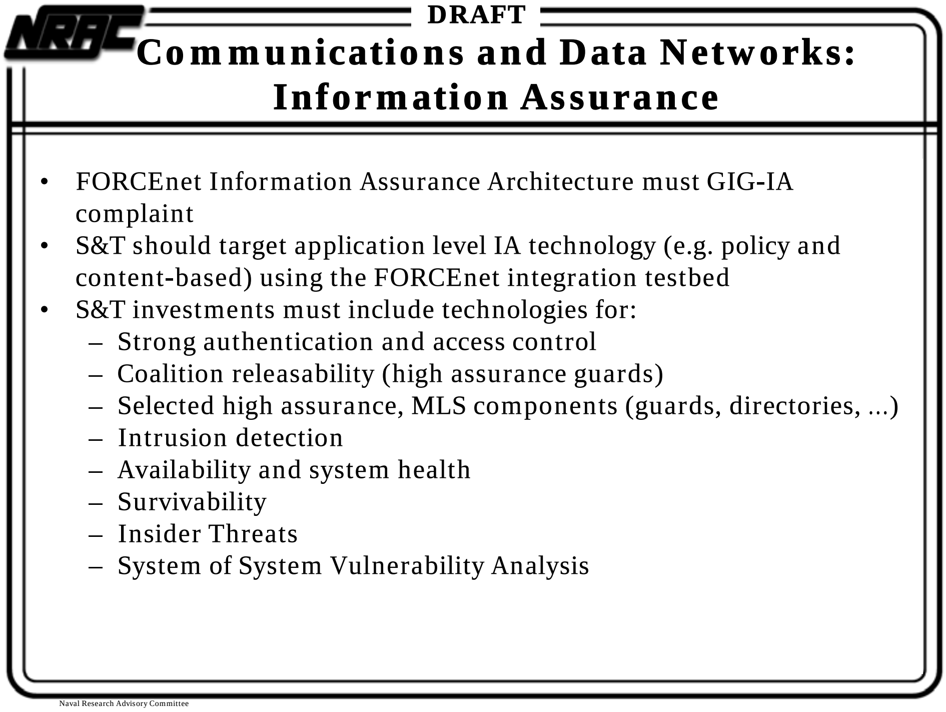


DRAFT

Persistent, Ubiquitous Connectivity is FORCEnet Prerequisite

- Naval Force components spread out beyond line of sight (BLOS) and require unique solutions
- SATCOM today for BLOS Comms
  - Non optimum antenna integration drives limited connectivity availability and limited data rates
- Persistent communications relay to provide over-the-horizon connectivity and link to GIG
  - High-Altitude Long-Endurance (HALE) UAV, space borne, E-2C, tanker, etc.
  - JTRS Wideband Networking Waveform (WNW) and MP-CDL (or “high-band version of WNW”) for BLOS connectivity
  - RF or lasercom extension to the GIG at all data rates via the Transformational Communications Architecture (TCA) satellites

Naval Research Advisory Committee

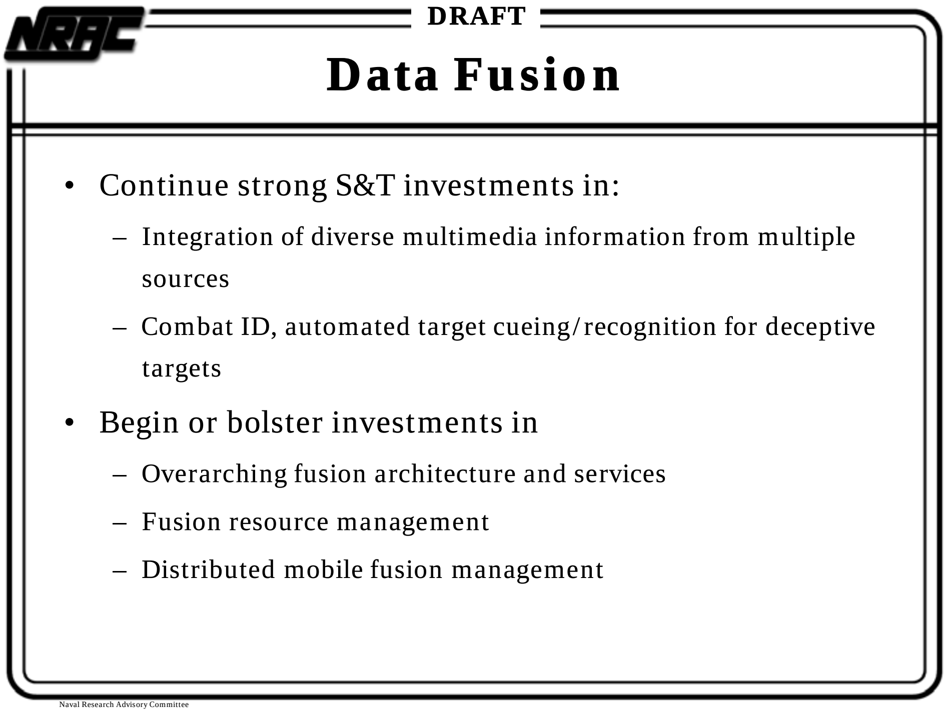


DRAFT

Communications and Data Networks: Information Assurance

- FORCEnet Information Assurance Architecture must GIG-IA complaint
- S&T should target application level IA technology (e.g. policy and content-based) using the FORCEnet integration testbed
- S&T investments must include technologies for:
  - Strong authentication and access control
  - Coalition releasability (high assurance guards)
  - Selected high assurance, MLS components (guards, directories, ...)
  - Intrusion detection
  - Availability and system health
  - Survivability
  - Insider Threats
  - System of System Vulnerability Analysis

Naval Research Advisory Committee

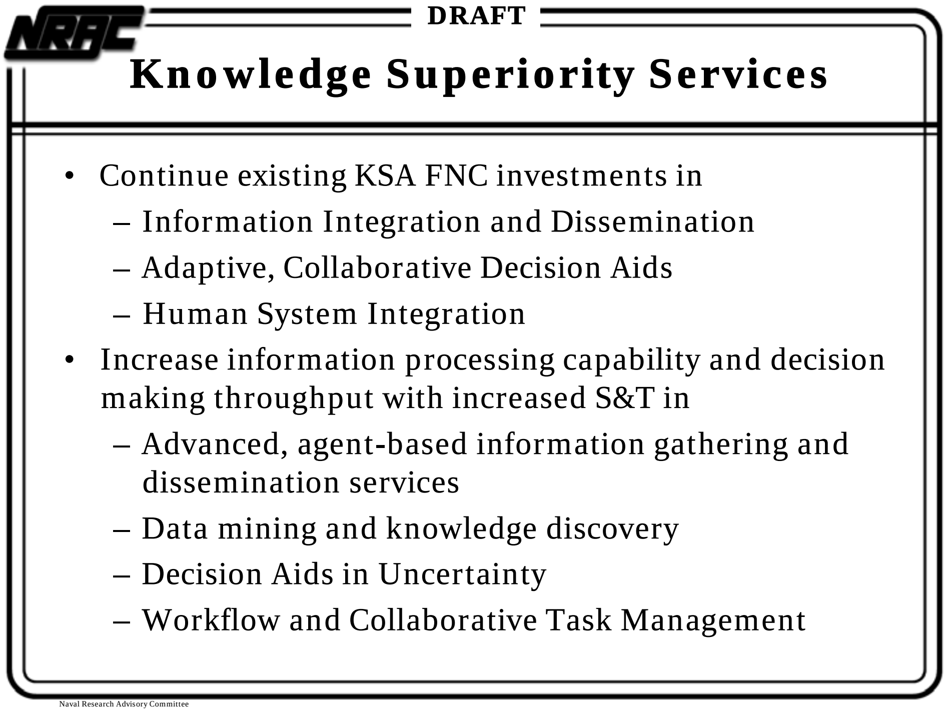


DRAFT

Data Fusion

- Continue strong S&T investments in:
  - Integration of diverse multimedia information from multiple sources
  - Combat ID, automated target cueing/recognition for deceptive targets
- Begin or bolster investments in
  - Overarching fusion architecture and services
  - Fusion resource management
  - Distributed mobile fusion management

Naval Research Advisory Committee

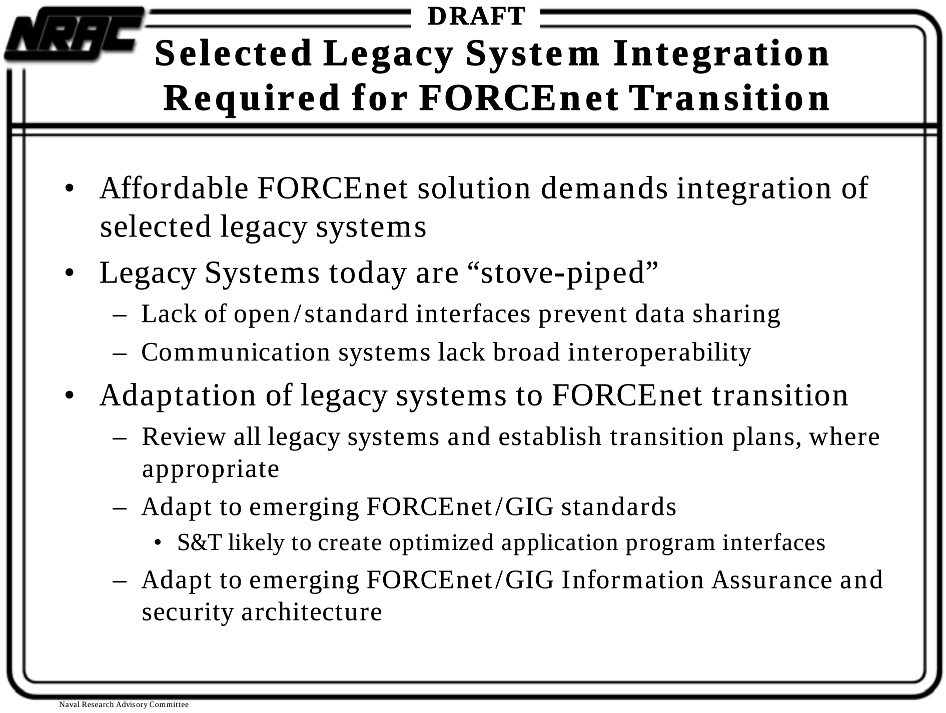


DRAFT

Knowledge Superiority Services

- Continue existing KSA FNC investments in
  - Information Integration and Dissemination
  - Adaptive, Collaborative Decision Aids
  - Human System Integration
- Increase information processing capability and decision making throughput with increased S&T in
  - Advanced, agent-based information gathering and dissemination services
  - Data mining and knowledge discovery
  - Decision Aids in Uncertainty
  - Workflow and Collaborative Task Management

Naval Research Advisory Committee



DRAFT

Selected Legacy System Integration Required for FORCEnet Transition

- Affordable FORCEnet solution demands integration of selected legacy systems
- Legacy Systems today are “stove-piped”
  - Lack of open/standard interfaces prevent data sharing
  - Communication systems lack broad interoperability
- Adaptation of legacy systems to FORCEnet transition
  - Review all legacy systems and establish transition plans, where appropriate
  - Adapt to emerging FORCEnet/GIG standards
    - S&T likely to create optimized application program interfaces
  - Adapt to emerging FORCEnet/GIG Information Assurance and security architecture

Naval Research Advisory Committee

This page intentionally left blank

APPENDIX D

ACRONYMS	DEFINITION
API	Application Programming Interfaces
ASN/RDA	Assistant Secretary of the Navy for Research, Development, and Acquisition
BAMS	Broad Area Maritime Surveillance
BCID	Baseline Initial Capabilities Document
BLOS	Beyond Light of Sound
CDN	Communications and Data Networks
CED	Capability Evolution Description
CMC	Commandant of the Marine Corp
CNO	Chief of Naval Operations
CNS	Core Network Services
COTD	Common Operational and Tactical Database
DARPA	Defense Advanced Research Projects Agency
DEP	Distributed Engineering Plant
DoD	Department of Defense
EMW	Expeditionary Maneuver Warfare
GIG	Global Information Grid
HIS	Human System Interface
IAS	Integrated Architecture and Standards
IS	Information Assurance
ISR	Intelligence, Surveillance and Reconnaissance
JTRS	Joint Tactical Radio System
KMT	Knowledge Management Tools
KSA FNC	Knowledge Superiority Assurance Future Naval Capability
M&S	Modeling and Simulation
NETWARMCOM	Naval Network Warfare Command
NRAC	Naval Research Advisory Committee
NRL	Naval Research Laboratory
NRO	Naval Reconnaissance Office
NSA	National Security Agency
ONR	Office of Naval Research
OSD	Office of the Secretary of Defense
PKI	Public Key Encryption
QoS	Quality of Service
R&D	Research and Development
S&T	Science and Technology
SATCOM	Satellite Communications
SECNAV	Secretary of the Navy
SPAWAR/ SPAWARSYSCOM	Space and Naval Warfare System Command
SYSCOM	Systems Command
TOR	Terms of Reference
UAV	Unmanned Aerial Vehicles

This page intentionally left blank